DECISION No MB/2021/17
# of the Management Board
# of the European Union Agency for Cybersecurity
(ENISA)
adopting the Programming Document 2022-2024, the Statement of estimates 2022 and the Establishment plan 2022

THE MANAGEMENT BOARD OF ENISA,

Having regard to the Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)[1], in particular Article 15.1.(c), Article 24.3., Article 24.4., and Article 29.7.

Having regard to the Decision No MB/2019/8 on the Financial Rules applicable to ENISA in conformity with the Commission Delegated Regulation (EU) No 2019/715 of 18 December 2018 of the European Parliament and of the Council.

Having regard to Commission Opinion (2021) 6130 final on the draft single programming document for 2022 – 2024 of ENISA dated 24.08.2021;

Having regard to Commission Communication C(2014) 9641 final, on the guidelines for programming document for decentralised agencies and the template for the Consolidated Annual Activity Report for decentralised agencies dated 16.12.2014;

Whereas:

(1) The Single Programming Document 2022-2024 should be adopted by the Management Board by 30 November 2021.

(2) The Single Programming Document 2022 -2024 was scrutinised by the Executive Board on 21-22 October 2021.

(3) The Programming Document of the Agency should be forwarded to the Member States, the European Parliament, the Council and the Commission following adoption;

[1] *OJ L 151, 7.6.2019, p. 15–69*

HAS DECIDED TO ADOPT THE FOLLOWING DECISION:

Article 1

The Single Programming Document 2022-2024, including ENISA International Strategy and the Annual Cooperation Programme with CERT-EU for 2022 is adopted as set out in the Annex 1 of this decision.

Article 2

The Statement of estimates of revenue and expenditure for the financial year 2022 and the Establishment plan 2022 is adopted as set-out in Annex 2 and Annex 3 of this decision. They shall become final following the definitive adoption of the general budget of the Union for the financial year 2022.

Article 3

Where necessary, the Management Board shall adjust ENISAs single programming document 2022-2024 and ENISA's budget and the Establishment plan in accordance with the general budget of the Union for the financial year 2022.

Article 4

The present decision shall enter into force on the day following that of its adoption. It will be published on the Agency's website.

Done at Athens on 17 November 2021.

On behalf of the Management Board,

[Signed]

Chair of the Management Board of ENISA

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ADOPTED SINGLE PROGRAMMING DOCUMENT 2022-2024

Including Multiannual planning,
Work programme 2022 and
Multiannual staff planning

VERSION: ADOPTED

TABLE OF CONTENTS

INTRODUCTION

FOREWORD

Europe's *digital decade* has started off with a wide range of key, ambitious and pioneering EU policy initiatives which will already lead to a changed digital landscape by the time we implement this ENISA 2022-2024 Single Programming Document.

A great many of these initiatives either directly or indirectly integrate cybersecurity concerns, challenges and solutions and they have been crowned in December 2020 by the EU's new Cybersecurity Strategy. ENISA is ready and indeed very proud to contribute to making these initiatives and their implementation a success, whether this be promoting the uptake of the EU's first cybersecurity certification schemes, revising the NIS Directive and the eIDAS Regulation, supporting the full implementation of the EU's 5G Cybersecurity Toolbox or fulfilling its respective roles within the Competence Centre and the Network or the new Joint Cyber Unit. It will use its new mandate, the expanded tasks and the fresh resources given to it by the Cybersecurity Act in 2019 to make sure that ENISA remains a key and reliable player and partner within the EU's cybersecurity ecosystem, able to tackle the ever-moving target of cybersecurity. It will furthermore make sure that the need for future resources is heard and remains tailored towards the EU's cybersecurity prerogatives.

In the second year of my tenure, I have been inspired in my work by the motivation and drive of the EU cybersecurity community - from my ENISA staff colleagues in their daily work to the political figureheads and the European stakeholder community in and across the EU and in the national institutions in their united vision and support. There is a real common determination and a *let's-do-it* approach to make Europe more cybersecure. We will need to maintain that momentum to tackle the ever-growing sophistication of cyber-attackers and cyber challenges. Only in this way we will be able to establish a European technological autonomy in the area of cybersecurity.

I am also particularly proud that - together with the Agency's staff and its Management Board - we have laid solid foundations to make ENISA more agile, more connected and more performance orientated in the way it works, and is reflected in the new organisational structure of ENISA and in the way we work, operational since 1st January 2021. This has been enshrined in the 2020 ENISA specific Strategy for a Trusted and Cyber Secure Europe. And the effects are showing, we are increasingly able to attract cybersecurity talent from all over the EU to help us make a difference. And with the generous support of our Greek host authorities, we have moved to larger premises in Athens, and are expanding our networks throughout the EU, specifically through the imminent opening of a local office in Brussels.

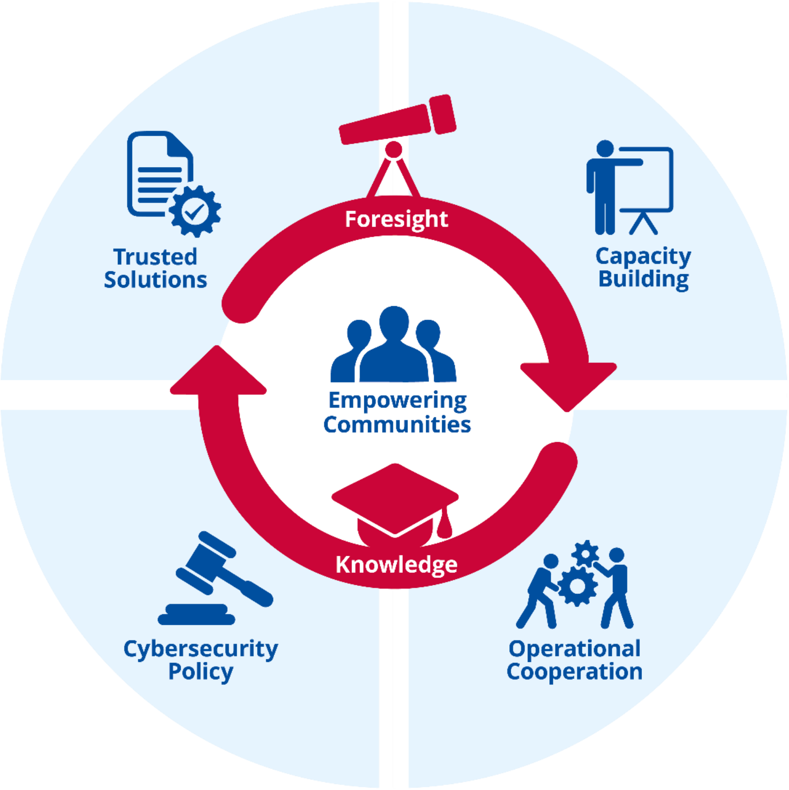
The full positive effects of these investments will only be truly felt once we have overcome the current pandemic, but I am convinced that we will come out of this stronger, more united and better prepared to embark on this European digital decade project.

Juhan Lepassaar

MISSION STATEMENT

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union in cooperation with the wider community. It does this through acting as a centre of expertise on cybersecurity, collecting and providing independent, high quality technical advice and assistance to Member States and EU bodies on cybersecurity. It contributes to developing and implementing the Union's cybersecurity policies.

Our aim is to strengthen trust in the connected economy, boost resilience and trust of the Union's infrastructure and services and keep our society and citizens digitally secure. We aspire to be an agile, environmentally and socially responsible organisation focused on people.



STRATEGY

EMPOWERING COMMUNITIES

Cybersecurity is a shared responsibility. Europe strives for a cross sectoral, all-inclusive cooperation framework. ENISA plays a key role in stimulating active cooperation between the cybersecurity stakeholders in Member States and the EU institutions and agencies. It strives to ensure complementarity of common efforts, by adding value to the stakeholders, exploring synergies and effectively using limited cybersecurity expertise and resources. Communities should be empowered to scale up the cybersecurity model.

CYBERSECURITY POLICY

Cybersecurity is the cornerstone of digital transformation and the need for it permeates all sectors, therefore it needs to be considered across a broad range of policy fields and initiatives. Cybersecurity must not be restricted to a specialist community of technical cybersecurity experts. Cybersecurity must therefore be embedded across all domains of EU policies. Avoiding fragmentation and the need for a coherent approach while taking into account the specificities of each sector is essential.

OPERATIONAL COOPERATION

The benefits of the European digital economy and society can only be fully attained under the premise of cybersecurity. Cyber-attacks know no borders. All layers of society can be impacted and the Union needs to be ready to respond to massive (large-scale and cross-border) cyber-attacks and cyber crisis. Cross-border interdependencies have highlighted the need for effective cooperation between Member States and the EU institutions for faster response and proper coordination of efforts at all levels (strategic, operational, technical and communications).

CAPACITY BUILDING

The frequency and sophistication of cyberattacks is rising speedily, while at the same time the use of ICT infrastructures and technologies by individuals, organisations, and industries is increasing rapidly. The needs for cybersecurity knowledge and competences exceeds the supply. The EU has to invest in building competences and talents in cybersecurity at all levels, from the non-expert to the highly skilled professional. The investments should focus not only on increasing the cybersecurity skillset in the Member States but also on making sure that the different operational communities possess the appropriate capacity to deal with the cyber threat landscape.

TRUSTED SOLUTION

Digital products and services bring benefits as well as risks, and these risks must be identified and mitigated. In the process of evaluating security of digital solutions and ensuring their trustworthiness, it is essential to adopt a common approach, with the goal to strike a balance between societal, market, economic and cybersecurity needs. A neutral entity acting in a transparent manner will increase customer trust on digital solutions and the wider digital environment.

FORESIGHT

Numerous new technologies, still in their infancy or close to mainstream adoption, would benefit from the use of foresight methods. Through a structured process enabling dialogue among stakeholders, decision- and policy-makers would be able to define early mitigation strategies that improve the EU resilience to cybersecurity threats and find solutions to address emerging challenges.

KNOWLEDGE

The energy that fuels the mill of cybersecurity is information and knowledge. For cybersecurity professionals to be efficient at tackling our objectives, to work in a constantly moving environment – in terms of digital developments as well as with regard to actors – to face the challenges of our time, a continuous process of collecting, organising, summarising, analysing, communicating, and maintaining cybersecurity information and knowledge is clearly needed. All phases are essential to ensure that information and knowledge is shared and expanded within the EU cybersecurity ecosystem.

SECTION I. GENERAL CONTEXT

2020 was characterised by the increased prioritisation of EU digital policies ranging from initiatives such as the Digital Services Act (DSA) to the cybersecurity-specific revision proposals of the NIS Directive – with many additional digital initiatives in between, such as the European Digital Identity. The EU's ambitions were coined by the phrase "making 2020-2030 'Europe's Digital Decade'" by Commission President Van der Leyen in her State of Union speech[1] in September 2020. Where cybersecurity is concerned, these ambitions were made more concrete in the EU's Cybersecurity Strategy[2] for the Digital Decade, released in December 2020 and also in the context of ensuring the EU's technological autonomy. This prioritisation continues in 2021[3] and beyond.

ENISA welcomes the EU's new Cybersecurity Strategy. The strategy proposes amongst many things, the review of the Network and Information Systems (NIS) Directive, a new Critical Entities Resilience (CER) Directive, a network of Security Operations Centres (SOCs), new measures to strengthen the EU Cyber Diplomacy Toolbox and the further implementation of the 5G Cybersecurity Toolbox. The Agency is ready to utilise fully its mandate and tasks to act in the areas outlined by the strategy which are covered by its mandate over the period of the SPD for 2022-2024.

The Covid-19 pandemic has not only brought healthcare challenges, it has also impacted the process of digitalization in Europe, worldwide and across sectors, has increased technological complexities and exposed the need to boost technology skill sets. These effects in turn have also accelerated the exposure to a wide range of cybersecurity threats and threat actors as documented by ENISA in 2021 on the one hand, while increasing the need for cybersecurity knowledge, awareness, resilience, cooperation and solutions on the other. This affects all aspects of the work of ENISA and the cybersecurity ecosystem that the EU is building up.

ENISA's 8th edition of its annual Threat Landscape Report[4] confirmed current and future trends that cyberattacks are becoming ever more sophisticated, targeted, widespread and undetected. Malware was voted again as the EU's number one cyber threat by a poll of intelligence experts, and changes were observed for phishing, identity theft and ransomware moving to higher-ranking positions. Monetisation remains cybercriminals' top motivation, and the COVID-19 environment fuelled attacks on homes, businesses, governments and critical infrastructure in 2020 and early 2021. Industries and governments alike continue to be hit by cyberespionage attacks. The number of data breach incidents continues to be very high, and the amount of stolen financial information and user credentials is growing. Unfortunately, we are getting used to hearing terms like *badrabbit ransomware, winnti, magecart* or *watering hole attacks*. In December 2020, the European Medicines Agency (EMA) was a victim of a cyberattack resulting in the leak of documents relating to the evaluation processes for COVID-19 vaccines. In the same month, another cyberattack to the software company SolarWinds through its supply chain resulted in a backdoor infiltration into its commercial software application. The list has continued into 2021, with further supply chain attacks with global implications such as Kaseya or SITA. The current escalation and the threat landscape status require ever new methods and a different approaches for Europe to become cyber secure.

[1] https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_1655
[2] https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391
[3] 15th September State of Union speech. And has been fortified by the most recent state of the union speech of 15 Sept which highlights the concepts of cooperation, resilience and situational awareness. https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_21_4701
[4] https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020

The adoption and implementation of policy frameworks is one key area where the EU is making a difference. Indeed, the policies and initiatives being put in place in the coming years will determine how the EU faces the cybersecurity challenges of today and tomorrow. Within this picture, ENISA will determine and adapt its support in particular in the following areas:

NIS2 & Joint Cyber Unit

Improving cyber resilience, particularly for those who operate essential services such as healthcare and energy or for those who provide online marketplace services has been the main focus of the current NIS Directive since 2016. The proposed expansion of scope under the new NIS2 Directive foresees far more entities obliged to take measures to increase the level of cybersecurity in Europe.

A 2020 ENISA study on NIS Investments[5] showed that for organisations implementing the NIS Directive "Unclear expectations" (35%) and "Limited support from the national authority" (22%) were among the challenges faced. The NIS2 proposal addresses these areas, aiming to provide more clarity towards what is expected from the national authorities, computer security incident response team (CSIRTs) and essential and important entities in terms of reporting, crisis management framework and information sharing.

ENISA is already invested in the above, with its resilience, cooperation and capacity-building work, and will be building up its own capacities to support the outcome of the proposal in the coming years using existing resources and building on these wherever necessary. This will also apply to increased cooperation under the potential Joint Cyber Unit umbrella. ENISA will contribute to the implementation of the Recommendation on 'building the Joint Cyber Unit', with a view to contributing to establishing an EU crisis management framework. This includes fostering cooperation among cybersecurity communities, among relevant EU institutions, bodies and agencies as well as within civilian (and between) cooperation networks (i.e. CyCLONe, CSIRTs Network and, to the extent needed, Cooperation Group).

Implementation of the EU cybersecurity certification framework

ENISA is playing a central role in supporting the implementation of the European cybersecurity certification framework by preparing and maintaining the candidate schemes with the support of area experts and in collaboration with public authorities in the Member States. It is expected that the draft candidate cybersecurity certifications schemes proposed by ENISA will be adopted as Commission implementing Regulations. The adopted schemes will allow a conformity assessment of digital products, services and processes in the Digital Single Market under those schemes, therefore increasing their cybersecurity. Currently, ENISA has prepared a candidate scheme on Common Criteria (EUCC) and is advancing its work on Cloud Services (EUCS) and 5G (EU5G).

Finalizing the candidate schemes for the more specialized product categories under the EUCC (EU Common Criteria) scheme and for cloud services is just the first step and should start bringing first benefits in terms of EU-wide certification processes and higher consumer and user trust during the time period 2022-2024.

[5] https://www.enisa.europa.eu/publications/nis-investments

Research & Innovation

The EU is extending its support and investments in the wealth of expertise and experience in cybersecurity research, technological and industrial development that exists in the Union also by prioritising cybersecurity in its research and innovation support efforts, and in particular through its Horizon Europe and Digital Europe programmes. It is also pooling resources and expertise by setting up the Competence Centre and the Network[6]. ENISA is ready to contribute to this essential area in the coming years within the role which has been given to it by the Regulation establishing the Competence Centre and the Network and by the mandate of the Cybersecurity Act. Some of this work can already be anticipated for the 2022-2024 period, and will be made more concrete as the Competence Centre is rolled out.

Artificial Intelligence (AI)

With the EU's AI agenda advancing rapidly following the European Commission proposal on AI[7] and Coordinated Plan on Artificial Intelligence 2021[8], the EU is addressing the major technological, ethical, legal and socio-economic challenges to put AI at the service of European citizens and the economy, for instance by considering linking high-risk AI systems to mandatory trustworthiness requirements. One of these challenges is understanding the interplay between cybersecurity and AI and how this can affect availability, safety or resilience of future AI services and applications.

Building on ENISA's AI Threat Landscape Report[9] of December 2020 and with the guidance from its Ad Hoc Expert Group on AI[10], the Agency can continue its open dialogue with EU institutions in support of the legislative initiatives reaching into 2022-2024. Here ENISA could continue supporting the Commission and Member States by providing good security practices and guidelines.

The European Digital Identity Framework

The EU's eIDAS regulation provides a framework for interoperability of national e-ID schemes and sets up an EU-wide market of (electronic) trust services. Electronic identity schemes and trust services are crucial for the EU digital market, because they allow citizens and businesses to carry out transactions online in a safe and trusted way. In 2020 the Commission reviewed the eIDAS Regulation and identified several gaps. In June 2021 the Commission adopted a proposal for a revised legal framework establishing a European Digital Identity[11], that can be used by all EU citizens and by EU businesses when carrying out online transactions. In the 2022-2024 period, ENISA will support Member States and the Commission in the implementation and the development of the toolbox and the European Digital Identity Framework as set out in Commission Recommendation of 3.6.2021[12] in addition to promoting the exchange of good practises and capacity building of relevant stakeholders.

Further developments

In 2020 ENISA put forward a proposal to open a local office in Brussels in accordance with CSA Art 20 (5). This will fortify ENISA's position in the digital ecosystem of the Union and in particular its role in

[6] Regulation (EU) 2021/887 of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres
[7] Proposal for a Regulation (EU) 2021/ 206 of 21 April 2021 laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts
[8] https://digital-strategy.ec.europa.eu/en/library/coordinated-plan-artificial-intelligence-2021-review
[9] https://www.enisa.europa.eu/news/enisa-news/enisa-ai-threat-landscape-report-unveils-major-cybersecurity-challenges
[10] https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/artificial_intelligence/ad-hoc-working-group
[11] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0281
[12] Commission Recommendation C(2001) 3968 of 3 June 2021 on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework.

establishing synergies with Union institutions, bodies, offices and agencies in the field of operational cooperation at the Union level. Moreover, the local office in Brussels aims to ensure regular and systematic cooperation with Union institutions, bodies and agencies and other competent bodies involved in cybersecurity. Indeed, it will support the delivery of tasks mandated to ENISA under Article 7 of the CSA, in particular that of establishing and maintaining structured cooperation with the Computer Emergency Response Team for the Union's institutions, bodies and agencies (CERT-EU). A detailed and annual cooperation plan is being integrated into ENISA's Single Programming Document and is part of the MoU signed in early 2021. Here both organizations will be able to benefit from synergies provided by proximity and daily contact and steer clear from any duplication of activities.

In 2021 ENISA established a cooperation agreement[13] with the European Telecommunications Standards Institute (ETSI). ETSI and ENISA have the common objective to collaborate, contribute to and promote, regional and international standardization . There is mutual interest in avoiding any duplication of technical work, and in adopting an aligned and complementary approach to the standardization process in specific domains.

[13] signature pending

SECTION II. MULTI-ANNUAL PROGRAMMING 2022 – 2024

Europe has for decades taken steps to improve digital security and trust through policies and initiatives. The Management Board of ENISA adopted a new strategy for the Agency in June 2020, which builds on the Cybersecurity Act (CSA), and outlines how the Agency will strive to meet the expectation of the cybersecurity ecosystem in a long-term perspective, in a manner that is open, innovative, agile as well as being socially and environmentally responsible. The strategy sets out a vision of "A trusted and cyber secure Europe" in which all citizens and organisations of Europe not only benefit but are also key components in the effort to secure Europe. Most importantly, the new ENISA strategy outlines seven strategic objectives which are derived from the CSA and set the expected long-term goals for the Agency.

1. Multi-annual work programme

The following table maps the strategic objectives stemming from ENISA's strategy[14], against the respective articles of the CSA. It furthermore integrates the activities of the Work Programme showing how the progress in the achievement of the objectives is monitored. These objectives may be reviewed through the ENISA Management Board as from 1st July 2024.

[14] The ENISA strategy entered into force on the 31 July 2020 and the Management Board shall launch a review procedure, if relevant, as from 1st July 2024.

STRATEGIC OBJECTIVE	ACTIONS TO ACHIEVE OBJECTIVE	ARTICLE OF THE CSA	EXPECTED RESULTS	KPI	METRICS [15]
SO1 **Empowered and engaged communities across the cybersecurity ecosystem**	Activities 1 to 9	Art.5 to Art.12	Empowered ecosystem encompassing Member States authorities, EU institutions, agencies and bodies, associations, research centres and universities, industry, private actors and citizens, who all play their role in making Europe cyber secure	Community-building across the cybersecurity ecosystem	Additional quantitative measures stemming from the stakeholder strategy that will be finalised in Q4 2021 Stakeholder satisfaction of ENISA's role as facilitator of community-building and collaboration across the cybersecurity ecosystem
SO2 **Cybersecurity as an integral part of EU policies**	Activities 1 & 2	Art.5	Cybersecurity aspects are considered and embedded across EU and national policies	ENISA's added value to EU institutions, bodies and Member States in providing support to policy-making (ex-ante)	1. Number of relevant contributions to EU and national policies and legislative initiatives 2. Number of references to ENISA reports, analysis and/or studies in EU and national policy documents 3. Satisfaction with ENISA added-value of contributions (survey)
			• Consistent implementation of Union policy and law in the area of cybersecurity • EU cybersecurity policy implementation reflects sectorial specificities and needs • Wider adoption and implementation of good practices	Contribution to policy implementation and implementation monitoring at EU and national level (ex-post)	1. Number of EU policies and regulations implemented at national level supported by ENISA 2 Number of ENISA reports, analysis and/or studies referred to at the EU and national level (survey) 3 Satisfaction with ENISA added-value of support (survey) [16]

[15] Baselines for these metrics should be known by the end of 2021, Therefore targets linked to these baselines will be developed for the 2023 work programme only in 2022.
[16] Surveys will be designed and developed in order to solicit a measurable response from participants to determine the added value of ENISAs contribution.

SO3 **Effective cooperation amongst operational actors within the Union in case of massive[17] cyber incidents**	Activities 4 & 5	Art.7	• All communities (EU Institutions and MS) use rationalised and coherent set of SOPs for cyber crises management • Efficient framework, tools (secure & high availability) and methodologies for effective cyber crisis management	Effective use of ENISA's tools, platforms and take up of SOPs in operational cooperation	1. Number of users both new and recurring and usage per platform/ tool/ SOPs provided by ENISA 2. Uptake of the platform/ tool/ SOPs during massive cyber incidents 3. Stakeholder satisfaction on the relevance and added value of the platforms/ tools/ SOPs provided by ENISA
			• Member States and institutions cooperating effectively during large scale cross border incidents or crises • Public informed on a regular basis of important cybersecurity developments • Stakeholders aware of current cybersecurity situation	ENISA ability and preparedness to support response to massive cyber incidents	1. Timeliness and relevance of information shared and expertise provided by ENISA in relation to incidents ENISA contributes to mitigate 2. Number of relevant incident responses ENISA contributed to as per CSA Art7 3.Stakeholders' satisfaction of ENISA's ability to provide operational support
SO4 **Cutting-edge competences and capabilities in cybersecurity across the Union**	Activities 3 & 9	Art.6 and Art.7(5)	• Enhanced capabilities across the community • Increased cooperation between communities	Increased resilience against cybersecurity risks and preparedness to respond to cyber incidents	1. Increase/decrease of maturity indicators 2. Outreach, uptake and application of lessons learnt from capability-building activities. 3. Number of cybersecurity programmes (courses) and participation rates 4. The number of exercises executed annually. 5. Stakeholder assessment on usefulness, added value an relevance of ENISA capacity building activities

[17] large scale and cross-border

		Art.10 & Art.12	• Greater understanding of cybersecurity risks and practices • Stronger European cybersecurity through higher global resilience.	Level of awareness on cybersecurity, cyber hygiene and cyber literacy across the EU Level of outreach	1. Number of cybersecurity incidents reported having human error as a root cause 2. Number of activities and participation to awareness raising actions organised by ENISA on cybersecurity topics 3. Geographical and community coverage of outreach in the EU 4. Level of awareness, on cybersecurity across the EU/ general public (e.g. EU barometer)
SO5 **High level of trust in secure digital solutions**	Activities 6 & 7	Art.8	Draft cybersecurity certification schemes developed by ENISA under the European cybersecurity certification framework are adopted Smooth transition to the EU cybersecurity certification framework Certified ICT products, services and processes are preferred by consumers and where relevant, Operators of Essential Services or Digital Service Providers	Uptake of the European cybersecurity certification framework and schemes as an enabler for secure digital solutions Effective preparation of candidate certification schemes prepared by ENISA	1. Number of stakeholders (governments or commercial solution providers) on the EU market using the cybersecurity certification framework for their digital solutions 2. Stakeholders trust in digital solutions of certification schemes (Citizens, public sector, businesses) 3. Uptake of certified digital solutions (products, services and processes) using certification schemes under the CSA framework 4. Number of candidate certification schemes prepared by ENISA 5. Number of people/organizations engaged in the preparation of certification schemes 6. Satisfaction with ENISA's support in the preparation of candidate schemes (survey)
			• Contribution towards understanding market dynamics • A more competitive European cybersecurity industry, SMEs and start-ups	Effectiveness of ENISAs supporting role for participants in the European cybersecurity market	1. Number of market analysis, guidelines and good practices issued by ENISA 2. Uptake of lessons learnt / recommendations from ENISA reports 3. Stakeholder satisfaction with the

					added value and quality of ENISA's work
SO6 **Foresight on emerging and future cybersecurity challenges**	Activity 8	Art.11 & Art. 9	• Research and innovation agenda tied to the cybersecurity needs and requirements, including contributing to the work of the European Cybersecurity Competence Centre	ENISA's ability to contribute to Europe's research and innovation agenda	1. Number of requests from Member States and EU research and innovation entities to contribute, provide advice or participate in activities. 2. Stakeholder satisfaction on the usefulness, relevance and timeliness of ENISA's foresight and advice on cybersecurity challenges & opportunities (incl in research)
SO7 **Efficient and effective cybersecurity information and knowledge management for Europe**	Activity 8	Art.9 & 11	• Decisions about cybersecurity are future proof and to take account the trends, developments and knowledge across the ecosystem • Stakeholders receive relevant and timely information for policy and decision making	ENISA's ability to contribute to Europe's cyber resilience through timely and effective information and knowledge	1. Number of users and frequency of usage of dedicated portal (observatory) 2 Number of recommendations, analysis, challenges identified and analysed 3 Stakeholder satisfaction on the usefulness, relevance and timeliness of ENISA's foresight and advice on cybersecurity challenges & opportunities (incl in research)

The strategy of ENISA also establishes a set of values which guide the execution of its mandate and its functioning, namely:

Community Mind-Set ENISA works with communities, respecting their competencies and expertise, and fosters synergies and trust to best achieve its mission.

Excellence ENISA aims for state-of-the-art expertise in its work, upholds the highest quality standards of operation and evaluates its performance to strive for continuous improvement through innovation and foresight.

Integrity/ethics ENISA upholds ethical principles and EU relevant rules and obligations in its services and working environment ensuring fairness and inclusiveness.

Respect ENISA respects fundamental European rights and values covering all its services and working environment, as well as the expectations of its stakeholders.

Responsibility ENISA assumes responsibility thus ensuring integration of the social and environmental dimensions into practices and procedures.

Transparency ENISA adopts procedures, structures and processes that are open, factual and independent, thus limiting bias, ambiguity, fraud and obscurity.

Those values are built on the ethos of the CSA, and in particular the objectives set out in Articles 3(4) and 4(1), and have been encapsulating into two corporate objectives, which form the baseline from which the multiannual activities of the SPD will be delivered.

The corporate objective of **sound resource and risk management** is derived from requirements in Art 4(1) of the CSA that sets an objective for the Agency to: “be a centre of expertise on cybersecurity by virtue of its independence, the scientific and technical quality of the advice and assistance it delivers, the information it provides, the transparency of its operating procedures, the methods of operation, and its diligence in carrying out its tasks”. In addition, the inspiration for this corporate objective stems from the values of **Excellence** and **Transparency** derived from the ENISA strategy and the principle of **Efficiency** set out in MB decision 2020/5 on the principles to be applied for organising ENISA. This aims for ENISA to uphold the highest quality of standards, strive for continuous improvement and enhance the organisation’s performance.

The corporate objective of **building an agile organisation focused on people** is derived from requirements in Art 3(4) of the CSA which obliges the Agency to: “develop its own resources, including /…/ human capabilities and skills, necessary to perform the tasks assigned to it under this Regulation”. In addition, the inspiration for this corporate objective stems from the values of **Responsibility** and **Respect** derived from the ENISA strategy and the principle of **Competences** set out in MB decision 2020/5 on the principles to be applied for organising ENISA. This aims for ENISA to respect fundamental European rights and values in its working environment, assume responsibility for social and environmental dimensions of its procedures and to develop its staff competences, expertise and talent.

CORPORATE OBJECTIVE	ACTIVITY TO ACHIEVE OBJECTIVE	ARTICLE OF THE CSA	EXPECTED RESULTS	KPI	METRICS
Sound resource and risk management	Activity 10	Art 4(1)	Maximize quality and value provided to stakeholders and citizens Building lasting credibility and trust	1.Organisational performance 2. Trust in ENISA brand	1. Proportion of KPI’s reaching targets 2. Individual contribution to achieving the objectives of the agency via clear link to KPI’s (CDR report) 3. Exceptions in Risk Register 4. Number of complaints filed against ENISA incl number of inquiries/ complaints of the EU Ombudsman 5. Number of complaints addressed timely and according to relevant procedures 6. Results of annual risk assessment exercise 7. Observations from external audit bodies (e.g. ECoA) requiring follow-up actions by

					ENISA (i.e. number of ‘critical’, ‘significant’ or ‘very important’ findings and number of observations successfully completed and closed 8. Level of trust in ENISA (survey)
Build an agile organisation focused on people	Activity 11	Art 3(4)	ENISA as an employer of choice	Staff commitment, motivation and satisfaction	1. Staff satisfaction survey (incl attractiveness of ENISA as employer, staff empowerment, organisational culture, opportunities on internal mobility, work-space, -environment and -tools) 2. Quantity and quality of ENISA training and career development activities organised for staff 3.Reasons for staff departure (exit interviews) 4.Staff retention/turnover rate 5.Resilience and quality of ENISA IT systems and services (including ability to consistently increase satisfaction with IT services & tools)

2. HUMAN AND FINANCIAL RESOURCES - OUTLOOK FOR YEARS 2022 – 2024

2.1 OVERVIEW OF THE PAST AND CURRENT SITUATION

Table 1

	2019	2020	2021	2022[18]
Number of posts in the Establishment Plan	59	69	76	82
% of fulfilment of the establishment plan (on 1st of January)	76%	80%	80%	94%

As an Agency, ENISA has historically always struggled to meet its human resources needs and take steps to ensure timely and rapid fulfilment of its Establishment Plan. The gap between the available posts and the fulfilment is evidenced in the table above. This has hampered the Agency to make use of its potential capabilities in the most efficient manner, resulting in a smaller real capacity of the Agency in terms of its human resources.

In order to change this, the Agency embarked in 2020 on a large-scale call for expression of interest for temporary agents (TA) and contract agents (CA) following a novel approach, with the aim of creating a sufficiently diverse and broad reserve shortlist of candidates with more transversal competences and skills that could be used to recruit staff thus fill the gaps in the current establishment plan, as well as serve as a pool of candidates for the establishment plan in multiannual basis. The call, which was accompanied by a widespread promotion campaign, attracted 1173 candidates for TA posts and 590 CA candidates and 229 manager candidates from across all Member States. This resulted in a reserve shortlist of 68 candidates for TA posts, for CA posts 15 and 8 manager posts in reserve shortlist. The charts below depicts the results of the recruitment exercise and the full table of results can be found in Annex IV table 4.

Fig.1 Recruited

[18] 3 AD posts subject to budget approval EC-NIS2 activities; projection of EP fulfilment on 01.01.2022 depends on successful conclusions of ongoing selections Q4 2021.

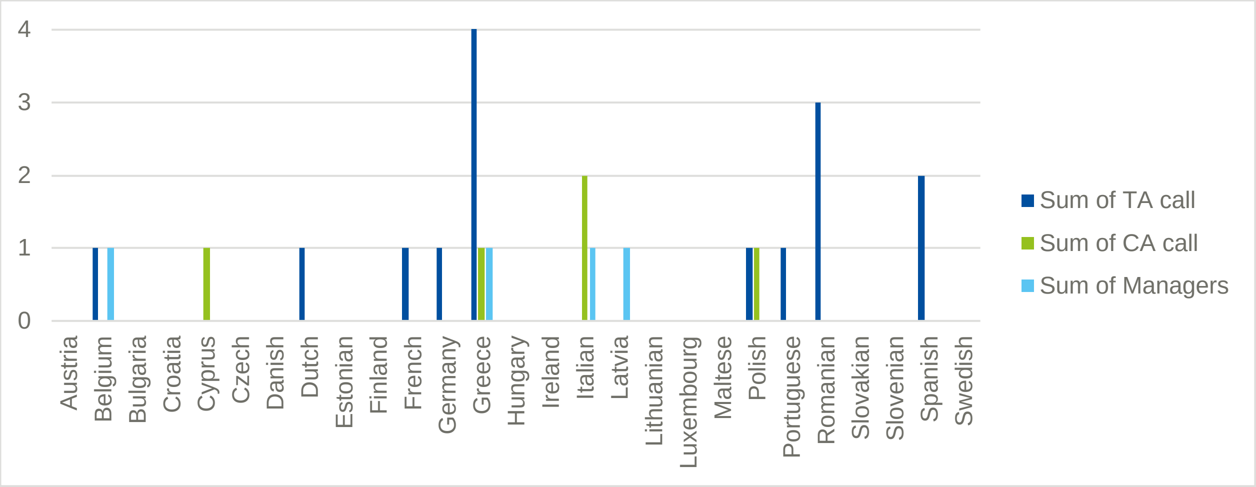
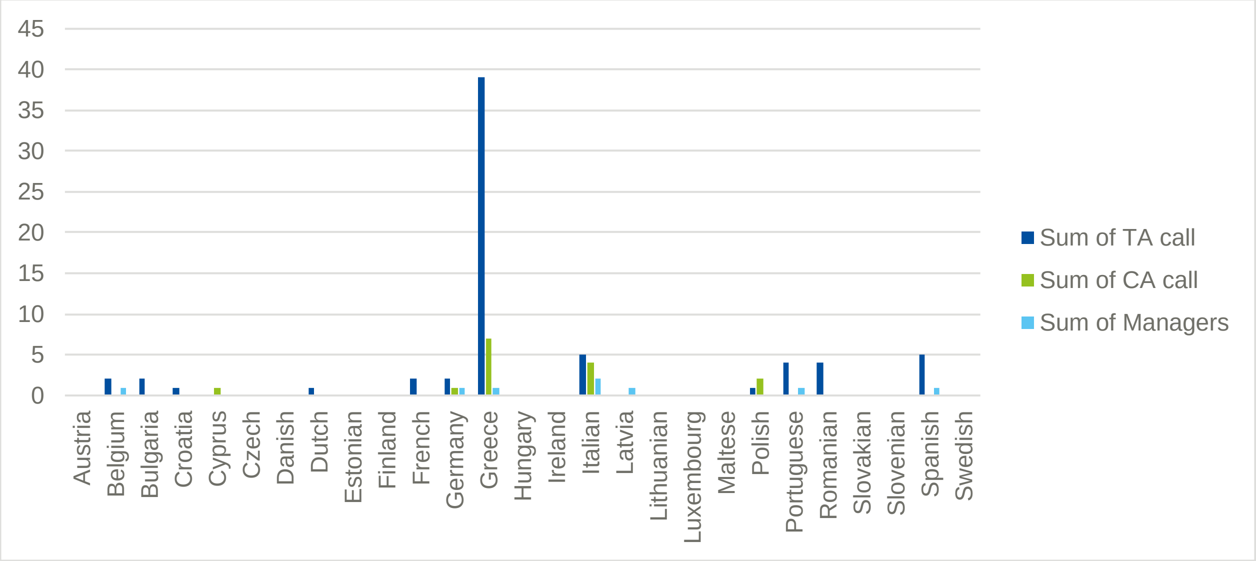


Fig.2 Reserve list



The second measure that the Agency put in place was to introduce an annual strategic workforce planning framework, which prompts the organisation to analyse its human resources needs ahead, on multiannual basis on the basis of the Single Programming Document, and plan and review the allocation of human resources between different activities as well as prepare new recruitment calls well in advance of the enactment of the applicable annual Establishment Plans. It also enables the Agency to take corrective action if and when necessary, to achieve the aims set out in Article 3(3) of the MB decision MB/2020/9, which foresees that the Executive Director will ensure that: “The average number of staff members assigned to the EDO and CSS [offices and services supporting the functioning of the Agency] shall not exceed the average number of staff members assigned to units [executing the objectives and tasks of the Agency].”

In the course of the 2021 Strategic Workforce Review, the Agency, along with other measures, reallocated altogether 4 posts from EDO and CSS, to be able to meet the threshold foreseen in Article 3(3) of MB/2020/9. This resulted in a termination of 1 contract and the prolongation of 2 contracts was put under review. The posts are now allocated to PDI, CBU and MCS, to be fulfilled via ongoing recruitment calls. The original impact that the conclusions of the 2021 Strategic Workforce Review was supposed to bring are summarised in the table below:

	Operational units		Supporting offices and services	
	Established staff	***average***	*Established staff*	***average***
Allocated as of 01.01.2021	48	**12**	38	**19**
Current allocation (01.10. 2021)	67	**16.75**	40	**20**
Projected allocation (01.01.2022)	79	**19.75**	40	**20**

2.2 OUTLOOK FOR THE YEARS 2022 – 2024

2.3 RESOURCE PROGRAMMING FOR THE YEARS 2022 – 2024

2.3.1 Financial Resources

The total EU contribution to ENISA over the period from 2022 to 2024, as well as for the full period of the new multiannual financial framework 2021–2027, is planned to remain stable, with a slight annual increase of circa 2% to reflect inflation (see the table below).

Table 2

	2021	2022 (*)	2023 (*)	2024 (*)
Total appropriations for ENISA *(thousand EUR)*	22 833[19]	24 208	24707	25220

Source: (*) Draft Union's annual budget for financial year 2022 COM (2021) 300 and Commission forecast including reserve budget EUR 610.000 due to NISD proposal

As from 2022, ENISA's revenue is composed of 97.6 % of ENISA's revenue from the EU contribution and 2.4 % was from the European Economic Area (EEA) country contribution (Table 6 in Annex III). In absolute terms, the EU and EEA contribution for 2022 is estimated respectively to reach EUR 23.6 million and EUR 0.6 million.

The general allocation of funds across titles is expected to remain stable over the period 2022–2024. Expenditure in 2022 is expected to amount to EUR 24.2 million, of which EUR 12.5 million in Title 1 covers all staff-related costs (52%), EUR 2.8 million in Title 2 covers main items such as building related expenditure and ICT expenses (11%) and EUR 8.9 million in Title 3 covers all core operating expenditure (37%). Total expenditures include the reserve

[19] Other contributions by the Hellenic authorities to cover rental payments for a maximum amount of EUR 640.000 are not included

budget of EUR 610 thousand expected to be allocated to cover additional staff (3 TAs and 2 CAs)[20] to manage part of the activities linked to the NIS directive in discussion by legislators.

2.3.2 Human Resources

In its budget proposal for the Single Programming Document (SPD) 2022 – 2024, the Agency asks for an extra 6 SNE posts introduced gradually 2+2+2 over 3 years). It stresses that the related costs would be budget-neutral; i.e. covered by ENISA's current budget and would therefore not imply any additional budgetary resources. ENISA proposes to cover the related costs through the established operational budget (Title 3)[21]; as the posts are directly linked to the operational needs and expectations of the Agency.

Specifically, the 6 additional SNE posts are crucial for the Agency's ability to address the tasks mandated by the Cybersecurity Act (CSA) in the areas of development of the National Cybersecurity Strategies, incident reporting, and indexing, but in particular in the area of operational cooperation (Article 7 CSA). They would therefore be justified both by the Agency's current activity areas, as well as by those extra activities and requirements, as foreseen especially in initial phases by the Commission's Recommendation on the Joint Cyber Unit (JCU) of 23 June 2021.

It is clear that the request for the 6 SNEs cannot cover all the potential future developments of the JCU, nor that only exclusively SNE posts will be able to cater for future needs. It is however also clear that without the inclusion of such posts, the Agency will be far more challenged to support the crucial initial phases of the JCU. Based on the above approach, the request for the 6 SNE posts without additional budgetary resources is made in a 3 year time-frame between 2022-2024 (e.g, they can be introduced gradually 2+2+2 over 3 years).

Finally, the collective knowledge acquired from MS perspective through such posts will be crucial for the success of these tasks. In fact, by importing unique expertise and knowledge into the Agency through SNE posts rather than having to outsource certain tasks or create any dependencies on other external staff, ENISA is catering for the increasing activities which require close cooperation with Member States as part of its mandate. Higher SNE turnovers will in turn be of direct benefit for all Member States and offer a rich experience to SNEs following their posting.

In addition, and pending the final outcome of the proposed NIS Directive initiative (NIS2)[22] as of 2022/23, ENISA may be tasked with additional action areas. While these action areas are covered by ENISA's general tasks according to its mandate, they would be supported by five (3 TAs and 2 CAs) supplementary FTEs with the corresponding budget of around €0,61M per year. This is an integrated part of the NIS2 proposal, subject to approval and managed as reserves that the Agency can draw on following the completion of the EU budget process

As all those resources are required in order to fulfil the operational mandate of the Agency, the Agency also plans to allocate all the new posts in operational units. Thus, although the current average does not meet the threshold foreseen in Article 3(3) of MB/2020/9, it should be regarded as a temporary derogation until such time as the new posts will become available and subsequently established. The Agency also commits itself not to raise the number of staff assigned to supporting offices and services (EDO and CSS) from its current level (a total of 40 staff members).

[20] the Commission asks ENISA to amend its establishment plan and resource planning in order to include the additional 5 full-time equivalents, 3 temporary agent and 2 contract agent posts, as specified in the legislative financial statement accompanying the proposal for a directive revising Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [(COM 2020/823) final]. These resources should be managed as reserves that the Agency can draw on once the final budget is adopted. The Commission invites the Agency to update the draft single programming document with the impact of this Commission Proposal.

[21] In terms of process at the time of writing the EC opinion of 24th August C(2021) 6130 did not support this proposal as reflected in the SPD22-24. This had been endorsed by the MB in the past and is currently pending final outcome in the budgetary approval process amongst co-legislators.

[22] Proposal COM 2020/823 of 16 December 2020 for a Directive revising Directive (EU) 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

2.4 STRATEGY FOR ACHIEVING EFFICIENCY GAINS

ENISA is committed to continuously implementing measures to obtain efficiency gains in all activities. In 2021 the ENISA organisational structure was implemented to follow the principles of sound budgetary management and build efficiencies in both executing its core mandate as well as in fulfilling its corporate functions. Also the Agency continues to implement its work programme by systematic use its statutory bodies (NLO Network, ENISA Advisory Group), as well as other statutory groups ENISA is involved in (SCCG as set out in CSA Art. 22, NISD Cooperation Group and its work-streams, expert groups created under the Union law) and its own ad hoc expert groups, where appropriate to peer-review the scope and direction of actions undertaken to implement outputs, as well as validate the results. This way the Agency will fulfil its obligation as outlined in Article 3(3) of the CSA, to avoid the duplication of Member State activities and taking into consideration existing Member State expertise. Hence, all activities enlisted under section 3.1. and 3.2. in this SPD contain an indication of how specific deliverables and other actions undertaken to fulfil the outputs will be validated and peer-reviewed or consulted as per legal framework in the area of certification.

In 2021 the framework for structured cooperation with CERT-EU to utilise synergies and avoid duplication of activities in executing its task in the field of operational cooperation (Art 7 of the CSA) is being implemented and a local office in Brussels established in 2021 should further enable the Agency to further create synergies with other EU Institutions, agencies and bodies within and beyond these activities. The Agency is also pursuing cooperation with relevant Union bodies (JRC) and will embark to create synergies with the Cybersecurity Competence Centre and Network once it is established to pursue synergies in fulfilling its tasks in the field of research and innovation (Article 11 of the CSA).

In its corporate functions, ENISA further seeks to rationalise its internal processes to improve its overall efficiency and to benchmark its activities with the best practices implemented by other EU Institutions and Agencies. The Agency is continuing and further expanding the sharing of services among other EU agencies. A number of collaborations and agreements are currently in place (EUIPO) and in 2021 the Agency signed a cooperation plan with EU-LISA.   In addition ENISA and CEDEFOP are strengthening their cooperation to streamline procurement, share financial services, increase efficiency gains in human resources, explore IT solutions together and to support each other in the area of data protection. The aim is to share knowledge and utilise human resources in the most efficient manner between the two agencies that results in better value for EU citizens.

Prompted by the COVID-19 crisis, the Agency established efficiency gains through digitalisation of its functions. It is already using the EU Tools such as ABAC; ABAC assets; Procurement; E-invoicing. Furthermore in 2020, the Agency deployed Sysper and in 2021 the migration of its services to other tools, such as MIPS and ARES are foreseen. Most of the administrative tasks are already supported by the application “Paperless” and others that are significant steps for the aimed 100% e-administration. E-trainings are also internally encouraged with the aim, among others, to reduce the associated costs from “class-room” training (traveling costs, etc…).

In 2021 the Agency has established a series of events and webinars to external parties and will upgrade its capabilities to use secure digital conferencing across the field, providing further opportunities in efficiency gains as well as expanding the scale and scope of its activities.

SECTION III. WORK PROGRAMME 2022

This is the main body of the Work Programme describing, per operational and corporate activity, what the agency aims to deliver in the respective year towards achieving its strategy and the expected results. In total nine operational activities and two corporate activities have been identified to support the implementation of ENISA's mandate in 2022.

The activities of the work programme seek to mirror and align with the tasks set out in chapter two of the CSA, demonstrating concretely not only the specific objectives, results and outputs expected for each task but also the resources assigned.

Activities one, two, three and nine represent the Agency's most mature areas with long standing projects such as policy support, Cyber Exercises and trainings and European Cybersecurity Month. Whilst activities four through to eight represent the areas of the Agency that are developing; such as contributing to cooperative response, certification, supporting the cybersecurity market and industry and finally providing analysis on emerging challenges. As such prioritisation in terms of resources are foreseen for these activities to support their development over the coming years.

In addition, the activities below do not reflect the additional five (3 TAs and 2 CAs) supplementary FTEs and the corresponding budget of €0,61M per year from the proposed NIS Directive initiative (NIS2)[23], this allocation will occur in due course and according to final agreement of regulators and once that tasks have been finalised.

[23] Proposal COM 2020/823 of 16 December 2020 for a Directive revising Directive (EU) 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

3.1 OPERATIONAL ACTIVITIES

Activity 1 Providing assistance on policy development

OVERVIEW OF ACTIVITY

The activity delivers assistance and advice to the EU and Member States in developing cybersecurity policy and sector-specific policy and law initiatives where matters related to cybersecurity are involved, and on the basis of the new 2020 EU Cybersecurity Strategy. While aspects such as privacy and personal data protection are taken into consideration (incl encryption).

The activity seeks to bolster policy initiatives on novel/emerging technology areas by providing technical, fact-driven and tailor-made cybersecurity advice and recommendations. In addition to support in emerging policy areas (such as AI, 5G, EU eID, quantum computing, blockchain, big data digital resilience and response to current and future crises). ENISA – in coordination with the EC and MSs will also conduct policy scouting to support them in identifying potential areas in policy development, as well as develop monitoring capabilities and tools to regularly and consistently be able to give advice on the effectiveness of the existing Union policy and law in accordance with the EU's institutional competencies in this area.

The added value of this activity is to support the decision makers in a timely manner on developments at the technological, societal and economic market levels which might affect the cybersecurity policy framework (see also Activity 8). Given the cross-cutting nature of cybersecurity across the policy landscape, the activity will provide an up-to-date risked based analysis of cybersecurity not only in the areas of critical infrastructure and sectors, but also by providingadvice across the field in an integrated and holistic manner. The legal basis for this activity is Article 5 of the CSA.

OBJECTIVES

- Foster cybersecurity as an integral part of EU policy (existing and new)
- Ensure that EU policy makers are regularly informed about the effectiveness of the existing frameworks and EU policy makers and stakeholders are provided with timely and tailor-made policy recommendations on future cybersecurity challenges and opportunities

RESULTS	LINK TO STRATEGIC OBJECTIVE (ENISA STRATEGY)
Cybersecurity aspects are considered and embedded across EU and national policies	Cybersecurity as an integral part of EU policies

OUTPUTS	KPI
1.1 Issue reports, studies and analyses on the effectiveness of the current cybersecurity policy frameworks 1.2 Carry out preparatory work and provide the EC and MSs with tailor-made advice and recommendations on new policy initiatives in emerging technological, societal and economic trends, such as Artificial Intelligence, 5G, eID, digital operational resilience in the finance sector and cyber insurance and other potential initiatives (e.g. The Once Only Technical Solution) 1.3 Assist the Commission in reviewing existing policy initiatives	**Indicator:** ENISA's added value to EU institutions, bodies and Member States in providing support to policy-making (ex-ante) **Metric:** 1.1 Number of relevant contributions to EU and national policies and legislative initiatives[24] 1.2 Number of references to ENISA reports, analysis and/or in EU and national policy documents 1.3 Satisfaction with ENISA added-value of contributions (survey) **Frequency:** Annual (1.1 & 1.2), biennial (1.3)

VALIDATION	TARGET GROUPS AND BENEFICIARIES
• NIS Cooperation Group (NIS CG) and other formally established Groups (outputs 1.1 & 1.2) • ENISA ad hoc working groups[25] (output 1.2) • NLO Network and ENISA Advisory Group and other formally established expert group (when necessary)	EU and national policy making institutions; EU and national experts (NIS CG, relevant/competent EU or MS-organisations/bodies) and of electronic communications services

RESOURCES PLANNED

Human Resources (FTE)			Financial Resources	EUR
Total	6[26]		Total	363000

[24] Baselines for these metrics should be known by the end of 2021, Therefore targets linked to these baselines will be developed for the 2023 work programme only in 2022.
[25] created under Art 20(4) of CSA
[26] Allocation of additional 5 FTEs from NIS proposal will occur in due course according to the final agreement of regulators and once the tasks have been finalised.

Activity 2 Supporting implementation of Union policy and law

OVERVIEW OF ACTIVITY

The activity provides support to MS and EU Institutions in the implementation of European cybersecurity policy and legal framework and advice on specific cybersecurity aspects related to the 2020 EU's Cybersecurity Strategy, NIS Directive, telecom and electronic communications security, data protection, privacy, eID including the European Digital Identity Framework and trust services, incident notification and the general availability or integrity of the public core of the open internet.

It further supports initiatives related to implementation of policy frameworks on novel digital technologies such as 5G (e.g. 5G Cybersecurity Toolbox) and assisting the work of the NIS Cooperation Group and its work streams.

Contribution towards the Commission's regular monitoring of the implementation of specific EU policies is envisaged, which considers relevant indicators and could contribute to possible indices which could capture the maturity of relevant cybersecurity policies, and provide input to the review of existing policies (Output 1.3)

This activity helps to avoid fragmentation and supports a coherent implementation of the Digital Single Market across Member States, following a consistent approach between cybersecurity, privacy and data protection.

The legal basis for this activity is Article 5 and Article 6 (1)b of CSA.

OBJECTIVES

- Consistent development of sectorial Union policies with horizontal Union policy to avoid implementation inconsistencies
- Contribute to the efficient and effective monitoring of EU cybersecurity policy implementation in MS
- Effective implementation of cybersecurity policy across the Union and aiming to support consistency of MS laws, regulations and administrative provisions related to cybersecurity
- Improved cybersecurity practices taking on board lesson learned from incident reports

RESULTS

- Consistent implementation of Union policy and law in the area of cybersecurity
- EU cybersecurity policy implementation reflects sectorial specificities and needs
- Wider adoption and implementation of good practices

Link to strategic objective (ENISA STRATEGY)

- Cybersecurity as an integral part of EU policies
- Empowered and engaged communities across the cybersecurity ecosystem

OUTPUTS

2.1 Support the NIS Cooperation Group and Work Streams as per NIS CG work programme and sectors under NISD

2.2 Support MS and Commission in the implementation and monitoring of the 5G Cybersecurity Toolbox and its individual actions

2.3 Provide advice, issue technical guidelines and facilitate exchange of good practices to support MS and EC on the implementation of cybersecurity policies in particular eID and the trust services framework, EECC and its implementing acts, as well as security measures for data protection and privacy

2.4 Assisting in establishing and implementing vulnerability disclosure policies considering also the NIS2 proposal.

KPI

Indicator: Contribution to policy implementation and implementation monitoring at EU and national level (ex-post)

Metric:

2.1 Number of EU policies and regulations implemented at national level supported by ENISA

2.2 Number of ENISA reports, analysis and/or studies referred to at the EU and national level (survey)

2.3 Satisfaction with ENISA added-value of support (survey)

Frequency: Annual (1), biennial (2 and 3)

VALIDATION

- NIS Cooperation Group or established work streams (output 2.1. 2.2.)
- Art19 and Art 13a expert groups (output 2.3.)
- Formally established bodies and expert groups as necessary (output 2.3, 2.4)
- NLO Network (as necessary)

TARGET GROUPS AND BENEFICIARIES

- MS Cybersecurity Authorities (NISD CG members), National Supervisory Authorities, Data Protection Authorities, National Accreditation Bodies
- EC, EU Institutions/ bodies (e.g. BEREC, EDPS, EDPB, ERA, EMSA) and sectorial EU Agencies (e.g. ACER) and Interinstitutional Committees (e.g. ICTAC, ICDT)
- Art. 13a and Art. 19 Expert Group members
- EU Citizens
- Conformity Assessment Bodies and Trust Service Providers
- Operators of Essential Services, including their associations and networks

RESOURCES PLANNED

Human Resources (FTE)			Financial Resources	EUR
Total	12		**Total**	798.475

Activity 3 Building capacity

OVERVIEW OF ACTIVITY

This activity seeks to improve and develop the capabilities of Member States, Union Institutions, bodies, and agencies, as well as various sectors, to respond to cyber threats and incidents, raise resilience and increase preparedness across the Union. Actions to support this activity include organising large scale exercises, sectorial exercises and trainings, including CSIRT trainings. In addition the activity seeks to develop and raise CSIRT capabilities, support information sharing within the cybersecurity ecosystem including cross-border, and assist in reviewing and developing national and Union level cybersecurity strategies,.

The legal basis for this activity is Articles 6 and 7(5) of the CSA.

OBJECTIVES

- Increase the level of preparedness and cooperation within and between Member States and sectors and EU institutions, bodies and agencies
- Prepare and test capabilities to respond to cybersecurity incidents
- Foster interoperable, consistent European risk management, methodologies and risk assessment practices
- Increase skill sets and align cybersecurity competencies
- Increase the supply of skilled professionals to meet market demand, and promote cybersecurity education

RESULTS

- Enhanced capabilities across the community
- Increased cooperation between communities

Link to strategic objectives (ENISA STRATEGY)

- Cutting-edge competences and capabilities in cybersecurity across the Union
- Empowered and engaged communities across the cybersecurity ecosystem

OUTPUTS

3.1 Assist MS to develop National Cybersecurity Strategies
3.2 Organise large scale biennial exercises and sectorial exercises (incl Cyber Europe, BlueOLEx, CyberSOPEx etc) including through cyber ranges
3.3 Organise trainings and other activities to support and develop maturity and skills of CSIRTs (incl. NIS sectorial CSIRT) and other communities
3.4 Develop coordinated and interoperable risk management frameworks
3.5 Support the capacity building activities of Cooperation Group and Work Streams as per NIS CG work programme
3.6 Support European Information Sharing communities through ISACs based on the Core service platform of CEF (Connecting Europe Facility), as well as other collaboration mechanisms such as PPPs. Support the reinforcement of SOCs as well as their collaboration, assisting the Commission and MS initiatives in this area in line with the objectives of the EU Cybersecurity Strategy in the building and improving of SOCs[27].
3.7 Organise and support cybersecurity challenges including European Cyber Security Challenge
3.8 Report on cybersecurity skills needs and gaps, and support skills development, maintenance and implementation (incl. Digital Education Action Plan and a report on higher-education programmes)

KPI

Indicator: increased resilience against cybersecurity risks and preparedness to respond to cyber incidents

Metric:

3.1 Increase/decrease of maturity indicators

3.2 Outreach, uptake and application of lessons learned from capability-building activities.
3.3 Number of cybersecurity programmes (courses) and participation rates
3.4 The number of exercises executed annually
3.5 Stakeholder assessment on usefulness, added value and relevance of ENISA capacity building activities. (Survey)

Frequency: 1, 2 3 & 4 Annual, 5 Biennial

VALIDATION

- NLO Network (as necessary)
- CSIRTs Network, (output 3.3.)
- CyCLONe members (as necessary)
- NIS Cooperation Group (output 3.5 and 3.6)
- Ad-hoc WG on SOCs (output 3.6)

TARGET GROUPS AND BENEFICIARIES

- Cybersecurity professionals
- EU Institutions and bodies
- Private industry sectors (operators of essential services such as health, transport etc.)
- CSIRTs Network and related operational communities
- European ISACs
- CyCLONe members

[27] In particular:
(a) Continue developing and updating the mapping of the current landscape of SOCs in the EU, incl. both public and private, in-house or as a service; main operators of SOCs services in the EU; Provide other relevant support to the Commission in implementing the SOCs- related objectives of the EU Cybersecurity Strategy (e.g. support to the design of calls for expression of interest, procurements, etc. liaison with stakeholders and research activities)
(b) Provide other relevant support to the Commission in implementing the SOCs- related objectives of the EU Cybersecurity Strategy (, e.g. support to the design of calls for expression of interest, procurements, etc. liaison with stakeholders and research activities.)

RESOURCES PLANNED				
Human Resources (FTE)			**Financial Resources**	EUR
Total	13		**Total**	1.921.265

Activity 4 Enabling operational cooperation

OVERVIEW OF ACTIVITY

The activity supports operational cooperation among Member States, Union institutions, bodies, offices and agencies and between operational activities inparticular by establishing a local office in Brussels, Belgium. Actions include establshing synergies with the different national cybersecurity communities (including the civilian, law enforcement, cyber diplomacy and cyber defence) and EU actors notably CERT-EU with the view to exchange know how, best practices, provide advice and issue guidance.

In addition the activity supports Member States with respect to operational cooperation within the CSIRTs network by advising on how to improve capabilities and providing support to ex-post technical inquiries regarding incidents.

Under this activity ENISA is supporting operational communities through helping to develop and maintain secure and highly available networks / IT platforms and communication channels in particular ensuring maintenance, deployment of the MeliCERTes platform.

In view of the EC Recommendation 4520 (2021) and Council Conclusions of the 20 October 2021 (ST 13048 2021) on 'exploring the potential of the Joint Cyber Unit initiative - complementing the EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises', ENISA will engage in the development of the JCU, along the lines and the roles defined according to on-going discussions amongst MS and EU operational actors.

The legal basis for this activity is Article 7 of the CSA.

OBJECTIVES

- Enhance and improve incident response capabilities across the Union
- Enable effective European cybersecurity crisis management by continuously improving the cyber crisis management framework
- Ensure coordination in cybersecurity crisis management among relevant EU institutions, bodies and agencies (e.g. CERT-EU, EEAS, EUROPOL)Improve maturity and capacities of operational communities (incl CSIRTs network, CyCLONe group)
- Contribute to preparedness, shared situational awareness and coordinated response and recovery to large scale cyber incidents and crises across different communities

RESULTS	Link to strategic objectives (ENISA STRATEGY)
• All communities (EU Institutions and MS) use rationalised and coherent set of SOPs for cyber crises management • Efficient framework, tools (secure & high availability) and methodologies for effective cyber crisis management	• Effective cooperation amongst operational actors within the Union in case of massive cyber incidents • Empowered and engaged communities across the cybersecurity ecosystem

OUTPUTS	KPI
4.1. Support the functioning and operations of the CSIRTs Network (also through MeliCERTes), CyCLONe, JCU, SOCs Network[28] and Cyber Crisis Management in the EU including cooperation with relevant Blueprint stakeholders (e.g Europol, CERT EU, EEAS and EDA) 4.2. Develop and enhance standard operating policies, procedures, methodologies and tools for cyber crisis management (also related to a future JCU). 4.3 Deploy and maintain operational cooperation platforms and tools (MeliCERTes, CyCLONe, MOU, etc) including preparations for a secure virtual platform for a future JCU	**Indicator:** Effective use of ENISA's tools, platforms and take up of SOPs in operational cooperation **Metric:** 4.1Number of users both new and recurring and usage per platform/ tool/ SOPs provided by ENISA 4.2 Uptake of the platform/ tool/ SOPs during massive cyber incidents 4.3 Stakeholder satisfaction on the relevance and added value of the platforms/ tools/ SOPs provided by ENISA. (Survey) **Frequency:** 1 & 2 annual and 3 biennial

VALIDATION	TARGET GROUPS AND BENEFICIARIES
• NLO Network (as necessary) • CSIRTs Network and CyCLONe (output 4.1.) • Blueprint actors	• Blueprint stakeholders • EU decision makers, institutions, agencies and bodies • MS CSIRTs Network Members • NISD Cooperation Group • OESs and DSPs

RESOURCES PLANNED

Human Resources (FTE)		**Financial Resources**	EUR

[28] Provide support for the design and development of cross-border platforms for pooling of CTI data at EU level (incl. definition of a blueprint architecture, data infrastructure requirements, data processing and analytics tools, data sharing protocols) CTI exchange initiatives already working; legal aspects; interoperability, etc.

Total	10		**Total**	1.703.350

Activity 5 Contribute to cooperative response at Union and Member States level

OVERVIEW OF ACTIVITY

The activity contributes to developing a cooperative response at Union and Member States level to large scale cross border incidents or crises related to cybersecurity by aggregating and analyzing reports to establish a common situational awareness, ensuring information flow and escalation measures between CISRTs network and technical, operational and political decision makers at Union level .

In addition, the activity can include, at the request of Member states facilitating the handling of incident or crises, public communication related to such incidents or crisis and testing cooperation plans for such incidents or crises. Supporting Union institutions, bodies, offices and agencies in public communication to incidents and crises. The activity also supports Member States with respect to operational cooperation within the CSIRTs network by providing advice to a specfic cyber threat, assisting in the assessment of incidents, facilitating technical handling of incidents, supporting cross-border information sharing and analyzing vulnerabilities.

This activity supports operational cooperation, including mutual assistance and the situational awareness in the framework of the proposed JCU.

Moreover the activity seeks to engage with CERT-EU in structured cooperation (Annex XIII Annual Cooperation Plan). The legal basis for this activity is Article 7 of the CSA

OBJECTIVES

- Effective incident response and cooperation amongst Member States and EU institutions, incl cooperation of technical and political actors during incidents or crisis
- Common situational awareness on cyber incidents and crisis across the Union
- Information exchange and cooperation, cross layer and cross border between Member States and as well as with EU institutions

RESULTS

- Member States and institutions cooperating effectively during large scale cross border incidents or crises
- Public informed of important cybersecurity developments
- Stakeholders aware of current cybersecurity situation

Link to strategic objectives (ENISA STRATEGY)

- Effective operational cooperation within the Union in case of massive (large-scale, cross-border) cyber incidents
- Empowered and engaged communities across the cybersecurity ecosystem

OUTPUTS

5.1. Generate and consolidate information (incl to the general public) on cyber situational awareness, technical situational reports, incident reports, threats and support consolidation and exchange of information on strategic, operational, and technical levels

5.2. Support technical (including through MeliCERTes) and operational cooperation, incident response coordination and EU wide crisis communication during large-scale cross border incidents or crises

5.3. Initiate the development of a trusted network of vendors/suppliers

KPI

Indicator: ENISA ability and preparedness to support response to massive cyber incidents

Metric:

5.1 Timeliness and relevance of information shared and expertise provided by ENISA in relation to incidents ENISA contributes to mitigate (Survey)

5.2 Stakeholders' satisfaction of ENISA's preparedness and ability to provide operational support (Survey)

5.3 Number of relevant incident responses ENISA contributed to as per CSA Art.7

Frequency: 1 & 2 biennial, 3 annual

VALIDATION

- Blueprint actors

TARGET GROUPS AND BENEFICIARIES

- EU Member States (incl CSIRTs Network members and CyCLONe)
- EU Institutions, bodies and agencies
- Other type of CSIRTs and PSIRTs

RESOURCES PLANNED

Human Resources (FTE)			Financial Resources	EUR
Total	8		Total	824.500

Activity 6 Development and maintenance of EU cybersecurity certification framework

OVERVIEW OF ACTIVITY

This activity emcompasses actions to establish a European cybersecurity schemes by preparing and reviewing candidate European cybersecurity certification schemes in accordance with Article 49 of the CSA, at the request of the Commission or on the basis of the Union Rolling Work Program. Actions also include evaluating adopted certification schemes and participating in peer reviews. In addition the activity assists the Commission in providing secretariat of the ECCG, providing secretariat of the SCCG; ENISA also makes available and maintains a dedicated European cybersecurity certification website Article 50 of the CSA.

The legal basis for this activity is Article 8 and Title III Cybersecurity certification framework of the CSA.

OBJECTIVES

- Trusted ICT products, services and processes
- Increase use and uptake of European cybersecurity certification
- Efficient and effective implementation of the European cybersecurity certification framework

RESULTS

- Certified ICT products, services and processes are preferred by consumers and businesses

Link to strategic objectives (ENISA STRATEGY)

- High level of trust in secure digital solutions
- Empowered and engaged communities across the cybersecurity ecosystem

OUTPUTS

6.1. Drafting and contributing to the preparation and establishment of candidate cybersecurity certification schemes

6.2. Implementation and maintenance of the established schemes including evaluation of adopted schemes, participation in peer review etc.

6.3. Support the statutory bodies in discharging carrying out their duties with respect to governance roles and tasks

6.4. Development and maintenance of necessary tools for making effective use of the Union's cybersecurity certification framework (incl. certification website, the Core service platform of CEF (Connecting Europe Facility) for collaboration, and publication, promotion of the implementation of the cybersecurity certification framework etc.)

KPI

Indicator:

1. Uptake of the European cybersecurity certification framework and schemes as an enabler for secure digital solutions.

2. Effective preparation of candidate certification schemes prepared by ENISA

Metric:

6.1 Number of stakeholders (public authorities and/or commercial solution providers) on the EU market using the cybersecurity certification framework for their digital solutions

6.2 Stakeholders trust in digital solutions of certification schemes (citizens, public sector and businesses. (Survey)

6.3 Uptake of certified digital solutions (products, services and processes) using certification schemes under the CSA framework

6.4. Number of candidate certification schemes prepared by ENISA

6.5 Number of people/organizations engaged in the preparation of certification schemes

6.6 Satisfaction with ENISA's support in the preparation of candidate schemes (survey)

Frequency: 1,4,5 annual, 2, 3, 6 biennial

VALIDATION

- Ad hoc certification expert groups (output 6.1.)
- ECCG (6.1.-6.2.)
- European Commission (outputs 6.1.-6.3)
- SCCG (output 6.3. and 6.4.)

TARGET GROUPS AND BENEFICIARIES

- Public authorities, accreditation bodies at Member States & EU level, Certification Supervisory Authorities, Conformity Assessment Bodies,
- Product manufacturers and service providers who have an interest in EU schemes for the certification of ICT products and services (industry)
- The European Commission, other Institutions, Agencies and competent authorities (e.g. EDPB), public authorities in the Member States, the members of the ECCG and the SCCG

RESOURCES PLANNED

Human Resources (FTE)			Financial Resources	EUR
Total	11		**Total**	1.025.750

Activity 7 Supporting European cybersecurity market and industry

OVERVIEW OF ACTIVITY

The activity seeks to foster cybersecurity market (products and services) in the Union and the development of the cybersecurity industry and services, in particular SMEs and start-ups, to reduce dependence from outside the Union and to reinforce supply chains inside the Union. It involves actions to promote and implement 'security by design' and 'security by default' measures in ICT products, services and processes, including through standardisation. Actions to support this activity include compiling guidelines and good practices on cybersecurity requirements, facilitating the establishment and take up of European and international standards for risk management as well as performing regular analysis of cybersecurity market trends on both the demand and supply side including monitoring, collecting and identifying dependencies among ICT products, services and processes and vulnerabilities present therein. Platforms for collaboration among the cybersecurity market players, improve visibility of trustworthy and secure ICT solutions in the internal digital market.

In addition this activity supports cybersecurity certification by monitoring standardisations being used by European cybersecurity of certification schemes and recommending appropriate technical specifications where such standards are not available.

The legal basis for this activity is Article 8 and Title III Cybersecurity certification framework of the CSA.

OBJECTIVES

- Improve the conditions for the functioning of the internal market
- Foster a robust European cybersecurity industry and market

RESULTS

- Contribution towards understanding market dynamics.
- A more competitive European cybersecurity industry, SMEs and start-ups

Link to strategic objectives (ENISA STRATEGY)

- High level of trust in secure digital solutions
- Empowered and engaged communities across the cybersecurity ecosystem

OUTPUTS

7.1. Market analysis on the main trends in the cybersecurity market on both the demand and supply side

7.2. Monitoring developments in related areas of standardisation, analysis on standardisation gaps and establishment and take-up of European and international standards for risk management in relation to certification

7.3. Guidelines and good practices on cybersecurity certification requirements for ICT products, services and processes

7.4. Monitoring and documenting the dependences and vulnerabilities of ICT products and services

KPI

Indicator: Effectiveness of ENISAs supporting role for participants in the European cybersecurity market

Metric:

7.1 Number of market analysis, guidelines and good practices issued by ENISA
7.2 Uptake of lessons learnt / recommendations from ENISA reports
7.3 Stakeholder satisfaction with the added value and quality of ENISA's work (Survey)

Frequency: 1 and2 annual,3 biennial

VALIDATION

- SCCG (outputs 7.2. & 7.3.)
- ENISA Advisory Group (output 7.1.)
- NLO (as necessary)
- ECCG (7.4)

TARGET GROUPS AND BENEFICIARIES

- European ICT industry, SME's, start-ups, product manufacturers and service providers
- European standardisation organisations (CEN, CENELEC and ETSI) as well as international and industry standardisation organisations

RESOURCES PLANNED

Human Resources (FTE)			Financial Resources	EUR
Total	8		Total	373.800

Activity 8 Knowledge on emerging cybersecurity challenges and opportunities

OVERVIEW OF ACTIVITY

This activity shall provide strategic long-term analysis, guidance and advice on emerging technologies (such as in the area of artificial intelligence, quantum, distributed ledgers, cloud computing, edge computing, software development, etc). On the basis of risk management principles, the Agency will identify cyber threats, vulnerabilities and risks, and map threat landscapes and provides topic-specific as well as general assessments on the expected societal, legal, economic and regulatory impact, as well as targeted recommendations to Member States and Union institutions, bodies, offices and agencies. In addition to this the activity will continue its efforts in developing the EU cybersecurity index. The activity also seeks to identify and give advice on research and innovation needs and priorities in the field of cybersecurity, and contribute to strategic agenda setting for cybersecurity research and innovation.

A key new component of this activity will be the contribution to the work of the European Cybersecurity Industrial, Technology and Research Competence Centre and Network of National Coordination Centres ("Competence Centre and Network"). This will include contributing to the development of a comprehensive and sustainable Cybersecurity Industrial, Technology and Research Agenda, and the respective work programmes.

These activities leverage on expertise of relevant legal, regulatory, economic and society trends and data by aggregating and analysing information.

The legal basis for this activity is Article 9 ,Article 11 and Article 5(6) of the CSA.

OBJECTIVES

- Identify and understand future cybersecurity challenges and opportunities and assess the interlinks between cybersecurity and relevant disrupting technologies in current and future digital transformation
- Increase Member States' and Union's resilience and preparedness in handling future cybersecurity challenges and opportunities
- Increase knowledge and information for specialised cybersecurity communities
- Understanding the current state of cybersecurity across the Union
- Link cybersecurity needs with the EU research & innovation agenda in the field of cybersecurity

RESULTS	Link to strategic objectives (ENISA STRATEGY)
• Decisions about cybersecurity are future proof and take account of the trends, developments and knowledge across the ecosystem • Stakeholders receive relevant and timely information for policy and decision-making • Research and innovation agenda tied to the cybersecurity needs and requirements	• Foresight on emerging and future cybersecurity challenges • Efficient and effective cybersecurity information and knowledge management for Europe • Empowered and engaged communities across the cybersecurity ecosystem

OUTPUTS	KPI
8.1 Develop and maintain EU cybersecurity index 8.2 Collect and analyse information to report on the cyber threat landscapes 8.3 Analyse and report on incidents as required by Art 5(6) of CSA 8.4 Develop and maintain a portal (information hub), a one stop shop to organise and make available to the public information on cybersecurity, and establishment of procedural framework to support knowledge management activities maximising synergies with the European Cybersecurity Atlas 8.5 Foresight on emerging and future cybersecurity challenges and recommendations. 8.6 Contribute to the Union's strategic research and innovation agenda and programmes in the field of cybersecurity (annual report). 8.7 Advise on potential investment priorities (e.g. capacity building and market & industry) and emergent cyber technologies in particular supporting the activities of the Competence Centre and the Network	**Indicator:** ENISA's ability to contribute to Europe's cyber resilience through timely and effective information and knowledge including into research and innovation agenda **Metric:** 8.1 Number of users and frequency of usage of dedicated portal (observatory) 8.2 Number of recommendations, analysis, challenges identified and analysed 8.3 Number of requests from Member States and EU research and innovation entities to contribute, provide advice or participate in activities. 8.4 Stakeholder satisfaction on the usefulness, relevance and timeliness of ENISA's foresight and advice on cybersecurity challenges & opportunities including in research (Survey) **Frequency:** 1,2 & 3 annual, 4 b-annual

VALIDATION	TARGET GROUPS AND BENEFICIARIES
• NLO Network (as necessary) • ENISA Advisory Group (as necessary) • ENISA ad hoc working group (as necessary) • Formally established bodies and expert groups as necessary (output 8.3) • The European Cybersecurity Competence Centre and Network of National Coordination Centres and Competence Centre Governing Board (output 8.6 & 8.7)	• General public • Industry, research and academic institutions and bodies • Art. 13a and Art. 19 Expert Group members • EU and national decision making bodies and authorities • European Cybersecurity Competence Centre & Network

RESOURCES PLANNED

Human Resources (FTE)		Financial Resources	EUR

Total	10		**Total**	1.051.950

Activity 9 Outreach and education

OVERVIEW OF ACTIVITY

The activity seeks to raise the overall awareness of cybersecurity risks and practices. in cooperation with Member States, Union institutions, bodies, offices and agencies and EU's international partners, it aims to build an empowered global community which can counter risks in line with the values of the Union. Under this activity the Agency will be organising regular outreach campaigns, providing guidance on best practices and support coordination across MS on awareness and education.

The added value of this activity comes from building global communities of stakeholders which improve and enhance current practices in cybersecurity by harmonizing and amplifying stakeholder actions.

The activity will also seek to contribute to the Unions efforts to cooperate with third countries and international organisations on cybersecurity.

The legal basis for this activity are Articles 10 and 12 and Article 42 of the CSA.

OBJECTIVES

- Advance cyber-secure behaviour by essential service providers in critical sectors
- Elevate the understanding of cybersecurity risks and practices across the EU and globally
- Foster EU cybersecurity values and priorities

RESULTS

- Greater understanding of cybersecurity risks and practices
- Stronger European cybersecurity through higher global resilience

Link to strategic objectives (ENISA STRATEGY)

- Empowered and engaged communities across the cybersecurity ecosystem

OUTPUTS

9.1 Develop activities to enhance behavioural change by essential service providers in critical sectors (as defined by the NISD)
9.2 Promote cybersecurity topics, education and good practices in the basis of the ENISA stakeholders' strategy
9.3 Implement ENISA international strategy and outreach
9.4 Organise European cybersecurity month (ECSM) and related activities

KPI

Indicator:

Level of awareness on cybersecurity, cyber hygiene and cyber literacy across the EU

Level of outreach

Metric:

9.1 Number of cybersecurity incidents reported having human error as a root cause
9.2 Number of activities and participation in awareness raising actions organised by ENISA on cybersecurity topics
9.3 Geographical and community coverage of outreach in the EU
9.4 Level of awareness on cybersecurity across the EU/ general public (e.g. EU barometer and other)

Frequency: 1,2 & 3 annual, 4 biennial

VALIDATION

- Management Board (output 9.1. and 9.3.)SCCG (for certification related issues under output 9.2)
- NLO Network
- ENISA Advisory Group (outputs 9.1. and 9.2)

TARGET GROUPS AND BENEFICIARIES

- Public, businesses and organisations
- Member States, EU institutions, bodies and agencies
- International partners

RESOURCES PLANNED

Human Resources (FTEs)			Financial Resources	EUR
Total	5		Total	439.900

3.2 CORPORATE ACTIVITIES

Activities 10 to 11 encompass enabling actions that support the operational activities of the agency.

<table>
<tr><th colspan="2">Activity 10: Performance and risk management</th></tr>
<tr><th colspan="2">OVERVIEW OF ACTIVITY</th></tr>
<tr><td colspan="2">The activity seeks to achieve requirements set out in Art 4(1) of the CSA that sets an objective for the Agency to: “be a centre of expertise on cybersecurity by virtue of its <b>independence</b>, the scientific and technical <b>quality of the advice and assistance it delivers</b>, the information it provides, the <b>transparency of its operating procedures</b>, the <b>methods of operation</b>, and its <b>diligence in carrying out its tasks</b>”. This objective requires an efficient performance and risk management framework, which should be developed and implemented Agency wide.
Under this activity ENISA will confinue to enhance key objectives of the reorganisation, as described in the MB decision No MB/2020/5., including the need to adress the gaps in the Agency’s quality assessment framework, install proper and functioning internal controls and compliance checks, make best use of the internal resources of the Agency, impose of sound financial and budgetary management, and utilise internal and external synergies within ENISA. These aspects are addressed in the new organisational architecture, but should also be built into the daily operations of the Agency as guided by the Work Programme. Actions undertaken will ensure that Agency’s outputs add real value, through making performance and ex-post and ex-ante evaluation integral to the Work Programme througout its lifecycle, including by rigorous quality assurance through proper project management, internal peer-reviews and independent audits and validations. Gaps in skills and trainings as well as resource planning will be reviewed and mitigated. The Agency will carry out a risk assessment of its organisational activities and IT systems and propose mitigation measures. The Agency will associate its main business processes with information systems that serve these processes and will produce a single registry of corporate processes (SOPs).
The legal basis for this activity is Art 4(1) and Art 32 of the CSA, the latter of which strongly focuses on the sound financial management principle with a view to maximise value to stakeholders.</td></tr>
<tr><th colspan="2">OBJECTIVES</th></tr>
<tr><td colspan="2">• Increased effectiveness and efficiency in achieving Agency objectives
• To be fully compliant with legal and financial frameworks in our performance (build a culture of compliance)
• Protect the Agencies assets and reputation, while reducing risks
• Full climate neutrality of all operations by 2030</td></tr>
<tr><th>RESULTS</th><th>Link to corporate objective:</th></tr>
<tr><td>Maximize quality and value provided to stakeholders and citizens
Building lasting credibility and trust</td><td>Sound resource and risk management</td></tr>
<tr><th>OUTPUTS</th><th>KPI</th></tr>
<tr><td>10.1. Implementation of performance management framework
10.2. Implementation of communications strategy
10.3. Develop and implement risk management plans (including IT systems cybersecurity risk assessment, quality management framework and as well as relevant policies and processes.
10.4. Develop and monitor the implementation of Agency wide budgetary and IT management processes
10.5.. Implement single administrative practices across the Agency
10.6. Carry out an overarching audit on the CO2 impact of all operations of the Agency and develop and implement a targeted action plan</td><td><b>Indicator</b>: Organisational performance culture
<b>Indicator:</b> Trust in ENISA brand
<b>Metrics:</b>
1 Proportion of KPI’s reaching targets
2 Individual staff contribution to achieving the objectives of the agency via clear link to KPI’s (CDR report)
3. Exceptions in Risk Register
4. Number of complaints filed against ENISA incl number of inquiries/ complaints of the EU Ombudsman
5. Number of complaints addressed timely and according to relevant procedures
6. Results of annual risk assessment exercise
7. Observations from external audit bodies (e.g. ECoA) requiring follow-up actions by ENISA (i.e. number of ‘critical’, ‘significant’ or ‘very important’ findings and number of observations successfully completed and closed
8. Level of trust in ENISA (survey)
<b>Frequency:</b> 1 to 6 annual, 8 biennial</td></tr>
<tr><th>VALIDATION</th><th>TARGET GROUPS AND BENEFICIARIES</th></tr>
<tr><td>• Management Team
• Budget Management Committee
• IT Management Committee
• IPR Management Committee
• Staff Committee
• ENISA Ethics Committee</td><td>• Citizens
• All stakeholders of the Agency</td></tr>
</table>

Activity 11 Staff development and working environment

OVERVIEW OF ACTIVITY

This activity seeks to support ENISA aspirations as stipulated in Art 3(4) which obliges the Agency to: "*develop its own resources, including /…/ human capabilities and skills, necessary to perform the tasks assigned to it under this Regulation*".

Moreover, the impact of the pandemic has shed new light on remote working . The Agency will continue to look into flexible (50/50) working arrangements to better balance work requirements in a pragmatic manner.

The actions which will be pursued under this activity will focus on attracting retaining and developing talent and building ENISA's reputation as employer of choice and as an agile and knowledge based organisation where staff can evolve personally and professionaly, keeping staff engaged, motivated and with sense of belonging. The activity will seek to build an attractive workspace by establishing and maintain excellent working conditions (premises, layout of office space) and developing user-centric (tele)working and conferencing tools (incl IT systems and platfoms) delivering state of the art services and supporting ENISA's business owners and stakeholders in line with the Agency's objectives.

OBJECTIVES

- Engaged staff, committed and motivated to deliver, empowered to use fully their talent, skills and competences
- Digitally enabled work-place and environment (incl home work-space) which promotes performance and balances social and environmental responsibility

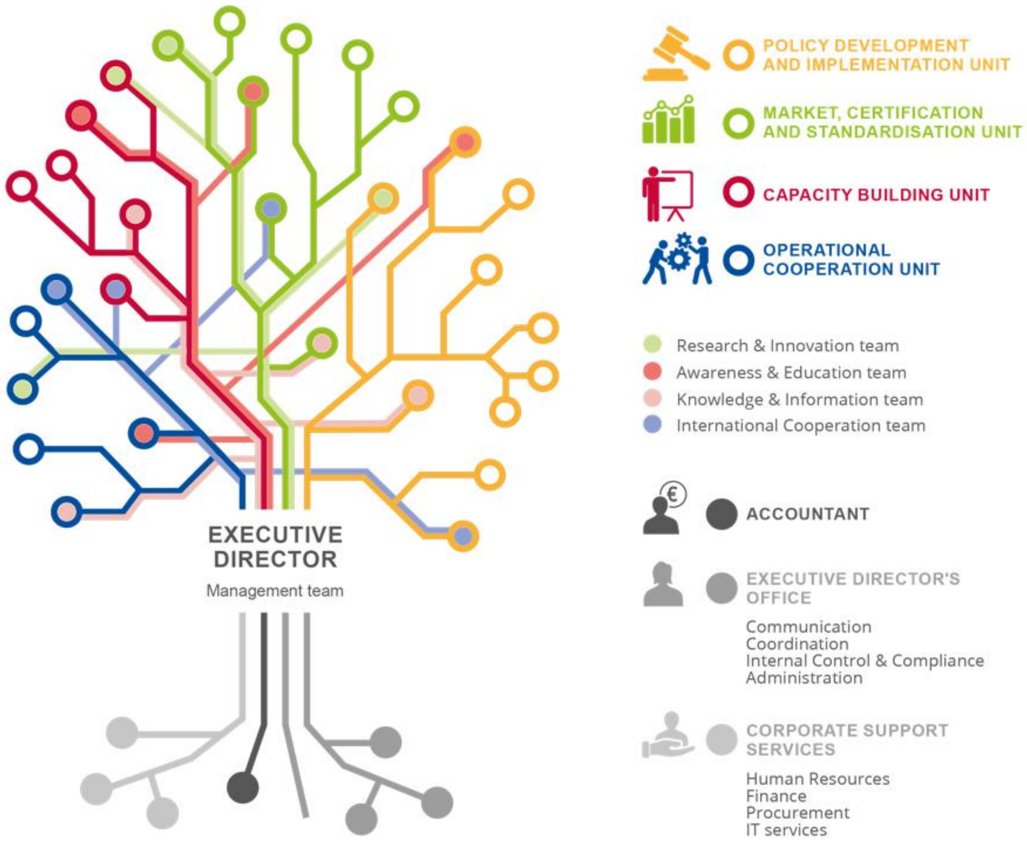
RESULTS	Link to corporate objective:
ENISA as an employer of choice	Build an agile organisation focused on people

OUTPUTS	KPI
11.1 Maintain and implement the competence framework into all HR processes (incl into training strategy, CDR, internal competitions, exit-interviews etc) 11.2 Develop HR Strategy with emphasis on talent development, growth and innovation 11.3 Undertake actions to develop and nourish talent and conduct necessary management development activities 11.4 Develop and maintain a user friendly and service oriented teleworking and office environment (including digital tools and services) 11.5 Set up service provisions standards and provide quality support and services for ENISA staff, employees, corporate partners and visitors	**Indicator** Staff commitment, motivation and satisfaction **Metric**: 11.1 Staff satisfaction survey (incl attractiveness of ENISA as employer, staff empowerment, organisational culture, opportunities on internal mobility, work-space, -environment and -tools) 11.2 Quantity and quality of ENISA training and career development activities organised for staff 11.3 Reasons for staff departure (exit interviews) 11.3 Staff retention/turnover rate 11.5 Resilience and quality of ENISA IT systems and services (including ability to consistently increase satisfaction with IT services & tools) **Frequency**: Annual (or ad hoc for metric no 11.3)

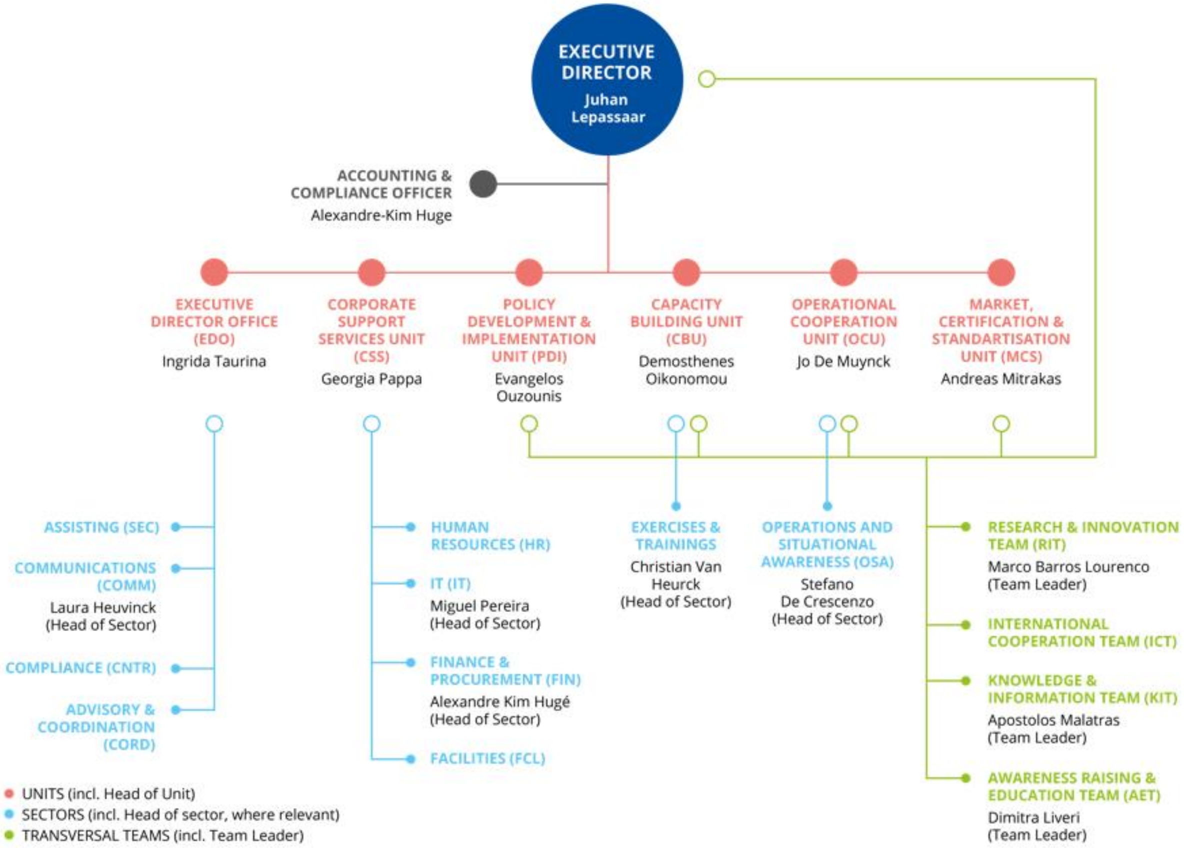
VALIDATION	TARGET GROUPS AND BENEFICIARIES
• Management Team • Joint Reclassification Committee • IT Management Committee • Task Force on relocation of the Agency • Staff Committee	• ENISA staff members and employees

ANNEX A

I. ORGANISATION CHART AS OF 01.01.2021


EXECUTIVE DIRECTOR
Management team
POLICY DEVELOPMENT AND IMPLEMENTATION UNIT
MARKET, CERTIFICATION AND STANDARDISATION UNIT
CAPACITY BUILDING UNIT
OPERATIONAL COOPERATION UNIT
Research & Innovation team
Awareness & Education team
Knowledge & Information team
International Cooperation team
ACCOUNTANT
EXECUTIVE DIRECTOR'S OFFICE
Communication
Coordination
Internal Control & Compliance
Administration
CORPORATE SUPPORT SERVICES
Human Resources
Finance
Procurement
IT services

Administrative Organigramme


EXECUTIVE DIRECTOR
Juhan Lepassaar
ACCOUNTING & COMPLIANCE OFFICER
Alexandre-Kim Huge
EXECUTIVE DIRECTOR OFFICE (EDO)
Ingrida Taurina
CORPORATE SUPPORT SERVICES UNIT (CSS)
Georgia Pappa
POLICY DEVELOPMENT & IMPLEMENTATION UNIT (PDI)
Evangelos Ouzounis
CAPACITY BUILDING UNIT (CBU)
Demosthenes Oikonomou
OPERATIONAL COOPERATION UNIT (OCU)
Jo De Muynck
MARKET, CERTIFICATION & STANDARTISATION UNIT (MCS)
Andreas Mitrakas
ASSISTING (SEC)
COMMUNICATIONS (COMM)
Laura Heuvinck
(Head of Sector)
COMPLIANCE (CNTR)
ADVISORY & COORDINATION (CORD)
HUMAN RESOURCES (HR)
IT (IT)
Miguel Pereira
(Head of Sector)
FINANCE & PROCUREMENT (FIN)
Alexandre Kim Hugé
(Head of Sector)
FACILITIES (FCL)
EXERCISES & TRAININGS
Christian Van Heurck
(Head of Sector)
OPERATIONS AND SITUATIONAL AWARENESS (OSA)
Stefano De Crescenzo
(Head of Sector)
RESEARCH & INNOVATION TEAM (RIT)
Marco Barros Lourenco
(Team Leader)
INTERNATIONAL COOPERATION TEAM (ICT)
KNOWLEDGE & INFORMATION TEAM (KIT)
Apostolos Malatras
(Team Leader)
AWARENESS RAISING & EDUCATION TEAM (AET)
Dimitra Liveri
(Team Leader)
● UNITS (incl. Head of Unit)
● SECTORS (incl. Head of sector, where relevant)
● TRANSVERSAL TEAMS (incl. Team Leader)

Status in-house staff (AD;AST;CA;SNEs) on 01.09.2021

	ED*	EDO	CSS	PDI	CBU	OCU	MCS	SUMMARY
AD	2	9	3	11	7	8	14	**54**
AST		8	6	0	2	0	0	**16**
CA		2	10	5	5	2,5	2,5	**27**
SNE		0	0	2	1	2	2	**7**
Total	**2**	**19**	**19**	**18**	**15**	**12,5**	**18,5**	**104**

* ED and accountant

II. RESOURCE ALLOCATION PER ACTIVITY 2022 - 2024

The indicative allocation of the total 2022 financial and human resources following the activities as described in part 3.1 in Section III and the corporate activities as described in part 3.2 in Section III are presented in the table[29] below. The allocation has been done following direct budget and FTEs indicated for each activity with indirect budget being assigned based on causal relationships.

The following assumptions are used in the simplified ABB methodology:

- Direct Budget is the cost estimate of each of the 9 operational activities and 2 corporate activities as indicated under Section 3 of the SPD 2022-2024 in terms of goods and services to be procured.
- Indirect Budget is the cost estimate of salaries and allowances, buildings, IT, equipment and miscellaneous operating costs, attributable to each activity. The indirect budget is allocated to activities based on different drivers. Main driver for costs allocation was number of foreseen FTEs for each activity in 2022.
- The allocation of 5 additional FTEs and EUR 610 thousand from the proposed NIS Directive will be allocated in due course according to the final agreement of regulators and once the tasks have been finalised.

[29] Pending final review

ALLOCATION OF HUMAN AND FINANCIAL RESOURCES (2022)	Activities as referred to in Section 3	Direct and Indirect budget allocation (in EUR)	FTE allocation
Providing assistance on policy development	Activity 1	1.034.117	6
Supporting implementation of Union policy and law	Activity 2	2.140.710	12
Building capacity	Activity 3	3.395.444	13
Enabling operational cooperation	Activity 4	2.852.015	10
Contribute to cooperative response at Union and Member States level	Activity 5	1.749.460	8
Development and maintenance of EU cybersecurity certification framework	Activity 6	2.367.985	11
Supporting European cybersecurity market and industry	Activity 7	1.268.623	8
Knowledge on emerging cybersecurity challenges and opportunities	Activity 8	2.282.332	10
Outreach and education	Activity 9	999.165	5
Performance and risk management	Activity 10	2.395.205	19
Staff development and working environment	Activity 11	3.112.569	19
TOTAL		**23.597.625**[30]	**121**[31]

[30] EUR 610 thousand foreseen under NIS directive will be allocated to activities in due course and according to final agreement of regulators including the finalised tasks

[31] Allocation of 5 FTEs from NIS directive will be allocated to activities in due course and according to final agreement of regulators and once the tasks have been finalised

III. FINANCIAL RESOURCES 2022 - 2024

Table 1: Revenue

REVENUES	2020 Executed Budget	2021 Revenue estimated by the agency	2022 As requested by the agency	VAR 2022 / 2021	Envisaged 2023	Envisaged 2024
1 REVENUE FROM FEES AND CHARGES						
2 EU CONTRIBUTION	20.646.000	22.248.000	23.633.000	6%	24.110.000	24.610.000
*- of which assigned revenues deriving from previous years' surpluses ***	*-110.505,47*					
- of which Reserve conditional to approval of NIS2 Directive			610.000		610.000	610.000
3 THIRD COUNTRIES CONTRIBUTION (incl. EEA/EFTA and candidate countries)	503.120	585.060	574.625	-2%	597.182	609.888
- of which EEA/EFTA (excl. Switzerland)	503.120	585.060	574.625	-2%	597.182	609.888
- of which Candidate Countries						
4 OTHER CONTRIBUTIONS	533.764	640.000	*	N/A		
5 ADMINISTRATIVE OPERATIONS						
- of which interest generated by funds paid by the Commission by way of the EU contribution (FFR Art. 58)						
6 REVENUES FROM SERVICES RENDERED AGAINST PAYMENT						
7 CORRECTION OF BUDGETARY IMBALANCES						
TOTAL REVENUES	**21.682.884**	**23.473.060**	**24.207.625**	**3%**	**24.707.182**	**25.219.888**

* - due to move to a new building, it is expected that Hellenic Authorities will make rental payments directly to the building owner, therefore no subsidy will be paid to ENISA

Table 2: Expenditure

EXPENDITURE	2021		2022	
	Commitment appropriations	**Payment appropriations**	**Commitment appropriations**	**Payment appropriations**
Title 1	10.775.409	10.775.409	12.494.335	12.494.335
Title 2	3.547.651	3.547.651	2.824.300	2.824.300
Title 3	9.150.000	9.150.000	8.888.990	8.888.990
Total expenditure	**23.473.060**	**23.473.060**	**24.207.625**	**24.207.625**

EXPENDITURE (in EUR)	Commitment and Payment appropriations					
	Executed budget 2020	Budget 2021	Draft Budget 2022 Agency request	VAR 2022 / 2021	Envisaged in 2023	Envisaged in 2024
Title 1. Staff Expenditure	**11.203.334**	**10.775.409**	**12.494.335**	**16%**	**12.740.555**	**12.998.652**
11 Staff in active employment *	7.126.084	8.810.319	10.837.880	23%	11.049.781	11.271.904
12 Recruitment expenditure	704.686	410.087	412.000	0%	420.536	429.483
13 Socio-medical services and training	375.738	1.084.064	853.000	-21%	870.672	889.197
14 Temporary assistance	2.996.826	470.939	391.455	-17%	399.565	408.067
Title 2. Building, equipment and miscellaneous expenditure	**3.150.568**	**3.547.651**	**2.824.300**	**-20%**	**2.882.814**	**2.944.150**
20 Building and associated costs	929.820	1.404.608	914.550	-35%	933.498	953.359
21 Movable property and associated costs	54.074	99.000	160.000	62%	163.315	166.790
22 Current corporate expenditure	98.702	798.696	320.000	-60%	326.630	333.579
23 Corporate ICT	2.067.972	1.245.347	1.429.750	15%	1.459.372	1.490.422
Title 3. Operational expenditure	**7.328.981**	**9.150.000**	**8.888.990**	**-3%**	**9.083.813**	**9.277.086**
30 Activities related to meetings and missions	628.966	650.000	387.000	-40%	395.018	403.423
32 Horizontal operational activities	1.517.962	0	0		0	0
36/37 Core operational activities	5.182.053	8.500.000	8.501.990	0%	8.688.795	8.873.663
TOTAL EXPENDITURE	**21.682.884**	**23.473.060**	**24.207.625**	**3%**	**24.707.182**	**25.219.888**

* for years 2022-2024 chapter 11 includes an amount of EUR 610 thousand as a reserve conditional to approval of NIS Directive (for salaries of new posts)

Table 3: Budget outturn and cancellation of appropriations

Budget outturn	2018	2019	**2020**
Revenue actually received (+)	11.572.995	16.740.086	21.801.460
Payments made (-)	-10.345.736	-11.980.352	-15.050.421
Carry-over of appropriations (-)	-1.348.657	-4.357.734	-6.200.614
Cancellation of appropriations carried over (+)	108.302	62.522	180.023
Adjustment for carry-over of assigned revenue appropriations carried over (+)	124.290	116.393	10.403
Exchange rate difference (+/-)	-689	-1.802	-1.291
Adjustment for negative balance from previous year (-)	-	-	-
Total	**110.505**	**579.113**	**739.560**

III.a Cancellation of appropriations

- Cancellation of Commitment Appropriations

In 2020, C1 Commitment Appropriations were cancelled for an amount of EUR 560 800 representing 3 % of the total budget. ENISA demonstrates a commitment rate of 97 % of C1 appropriations of the year at the year-end (31/12). The consumption of the 2020 budget at year-end shows the capacity of the Agency to fully implement its annual appropriations. The payment rate reached 69 % and the amount carried forward to 2021 is EUR 6 074 991 representing 29 % of total C1 appropriations in 2020.

- Cancellation of Payment Appropriations for the year

No payment appropriations were cancelled during 2020.

- Cancellation of Payment Appropriations carried over

(Fund source “C8” – appropriations carried over automatically from 2019 to 2020.)

The appropriations of 2019 carried over to 2020 were utilised at a rate of 96 % (automatic carry-overs) which indicates a satisfactory capability of estimation of needs. From the amount of EUR 4 347 332 carried forward, the amount of EUR 180 024 was cancelled, mostly due to the circumstances caused by COVID-19. This cancellation represents 0,7 % of the total budget 2020 (fund sources C1 and C8).

IV. HUMAN RESOURCES- QUANTITATIVE

Overview of all categories of staff and its evolution

Staff policy plan for 2022 - 2024

Table 1: Staff population and its evolution; Overview of all categories of staff

Statutory staff and SNE

STAFF	2021			2021	2022	2023	2024
ESTABLISHMENT PLAN POSTS	**Authorised Budget**	**Actually filled as of 01/09/2021**	**Occupancy rate %**	Authorised	Authorised[32]	**Envisaged staff**	Envisaged staff
Administrators (AD)	57	54[33]	95%	57	63[34]	63	63
Assistants (AST)	19	17[35]	89%	19	19	19	19
Assistants/Secretaries (AST/SC)							
TOTAL ESTABLISHMENT PLAN POSTS	76	71	93%	76	82	82	82
EXTERNAL STAFF	**FTE corresponding to the authorised budget 2021**	**Executed FTE as of 01/09/2021**	**Execution Rate %**	**FTE corresponding to the authorised budget**	**Envisaged FTE**	**Envisaged FTE**	Envisaged FTE
Contract Agents (CA)	30	27	90%	30	32[36]	32*	32*
Seconded National Experts (SNE)	12	9[37]	75%	12	12	12	12

[32] Pending approval of NIS directive and request for additional SNE posts subject to approval procedure between the co-legislators.
[33] Total AD includes 54 AD actually filled by 15.11.2021. Date of reference for the figures 16.09.2021.
[34] Additional 3 TA posts for implementation of NIS directive
[35] Total AST includes 17 AST actually filled by 01.10.2021. Date of reference for the figures 16.09.2021.
[36]* Additional 2 CA posts for implementation of NIS directive
[37] Total SNE includes 9 SNE filled by 01.10.2021. Data of reference 16.09.2021.

TOTAL External Staff	42	49	N/A	42	44	44	44
TOTAL STAFF[38]	118	107	91%	118	126[39]	126	126

Final statutory staff as of year end 31.12.2020

STAFF	2020		
ESTABLISHMENT PLAN POSTS	Authorised Budget	Actually filled as of 31/12/2020	Occupancy rate %
Administrators (AD)	51	47[40]	92%
Assistants (AST)	18	15	83%
Assistants/Secretaries (AST/SC)			
TOTAL ESTABLISHMENT PLAN POSTS	69	62	90%
EXTERNAL STAFF	FTE corresponding to the authorised budget	Executed FTE as of 31/12/2020	Execution Rate %
Contract Agents (CA)	30	29[41]	97%
Seconded National Experts (SNE)	12	8	67%
TOTAL EXTERNAL STAFF	5	31	100%
TOTAL	47	68	100%
TOTAL STAFF	116	130	100%

Additional external staff expected to be financed from grant, contribution or service-level agreements

Human Resources	2021	2022	2023	2024
	Envisaged FTE	Envisaged FTE	Envisaged FTE	Envisaged FTE
Contract Agents (CA)	n/a	n/a	n/a	n/a
Seconded National Experts (SNE)	n/a	n/a	n/a	n/a
TOTAL	n/a	n/a	n/a	n/a

[38] Refers to TA, CA and SNEs figures.

[39] This includes the additional 5 full-time equivalents, 3 temporary agent and 2 contract agent posts, as specified in the legislative financial statement accompanying the proposal for a directive revising Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [(COM 2020/823) . These resources should be managed as reserves that the Agency can draw on following the final EU budget adopted..

[40] Total number includes the in-house AD staff by 31/12/2020 and 9 AD offers sent and accepted by 31/12/2020.

[41] Total number includes the in-house CA staff by 31/12/2020 and 3 offers sent and accepted by 31/12/2020.

Other Human Resources

- Structural service providers

	Actually in place as of 31/12/2020	Actually in place as of 01/09/2021
Security	5	5
IT	4	5

- Interim workers

	Actually in place as of 31/12/2020	Actually in place as of 01/09/2021
Number	31	13

Table 2: Multi-annual staff policy plan Year , 2020, 2021, 2022, 2023, 2024[42]

Function group and grade	2020				2021				2022[43]		2023*		2024*	
	Authorised budget		Actually filled as of 31/12[44]		Authorised budget		Actually filled as of 01/09/2021[45]		Authorised		Envisaged		Envisaged	
	Permanent posts	Temporary posts	Permanent posts	Temp. posts	Perm. Posts	Temp. posts	Perm. Posts	Temp posts	Perm. posts	Temp. posts	Perm. posts	Temp. posts	Perm. posts	Temp. posts
AD 16														
AD 15		1				1				1		1		1
AD 14				1				1						
AD 13						1				2		2		2
AD 12		6		6		5		6		4		4		4
AD 11						2				2		2		2
AD 10		5		3		3		3		4		4		4
AD 9		12		7		12		9		11		11		11
AD8		19		10		21		10		23		23		23
AD 7				11		8		12		10		10		10
AD 6				9		4		13		6		6		6
AD 5														
AD TOTAL		43		47		57		54		63		63		63
AST 11														
AST 10														

[42] The change in the number of establishment plan up to 10% requested for year 2022 is modified as per Art 38 of the ENISA Financial Regulation. In 2022, ENISA will review its staffing strategy and will update a forecast for reclassification also in line with job mapping.
[43]* To be updated at a later stage during Q4 2021
[44] Total number includes the in-house AD staff by 31/12/2020 and 9 AD offers sent and accepted by 31/12/2020. Data available as of 01.01.2021 and refers to the take up duties.
[45] The figures include actually filled posts as of 15.11.2021 Date of reference for the figures 16.09.2021.

Function group and grade	2020				2021				2022[43]		2023*		2024*	
	Authorised budget		Actually filled as of 31/12[44]		Authorised budget		Actually filled as of 01/09/2021[45]		Authorised		Envisaged		Envisaged	
	Permanent posts	Temporary posts	Permanent posts	Temp. posts	Perm. Posts	Temp. posts	Perm. Posts	Temp posts	Perm. posts	Temp. posts	Perm. posts	Temp. posts	Perm. posts	Temp. posts
AST 9														
AST 8						1				2		2		2
AST 7		3		3		4		3		3		3		3
AST 6		7		1		8		2		8		8		8
AST 5		5		5		5		5		5		5		5
AST 4		1		3		1		4		1		1		1
AST 3				2				2						
AST 2				1				1						
AST 1														
AST TOTAL		16		15		19		17		19		19		19
AST/SC 6														
AST/SC 5														
AST/SC 4														
AST/SC 3														
AST/SC 2														
AST/SC 1														
AST/SC TOTAL														
TOTAL		59		62		76		71		82		82		82
GRAND TOTAL	59		62		76		71		82		82		82	

External personnel

Contract Agents

Contract agents	FTE corresponding to the authorised budget 2020	Executed FTE as of 31/12/2020	Headcount as of 31/12/2020	FTE corresponding to the authorised budget 2021	Executed FTE as of 01/09/2021[46]	FTE corresponding to the authorised budget 2022	FTE corresponding to the authorised budget 2023	FTE correspondin to the authorised budget 2024
unction Group IV	28	20[47]	20[48]	28	19	30[49]	30	30
unction Group III	2	8	8	2	7	2	2	2
unction Group II	0	0	0	0	0	0	0	0

[46] Contract Agents in-house including 01.09.2021. Date of reference for the figures 16.09.2021.

[47] Total number includes the in-house CA staff by 31/12/2020 and 3 offers sent and accepted by 31/12/2020.

[48] Total number includes the in-house CA staff by 31/12/2020 and 3 offers sent and accepted by 31/12/2020.

[49] This includes the additional 2 contract agent posts, as specified in the legislative financial statement accompanying the proposal for a directive revising Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [(COM 2020/823) . These resources should be managed as reserves that the Agency can draw on following the final EU budget adopted.

Contract agents	FTE corresponding to the authorised budget 2020	Executed FTE as of 31/12/2020	Headcount as of 31/12/2020	FTE corresponding to the authorised budget 2021	Executed FTE as of 01/09/2021[46]	FTE corresponding to the authorised budget 2022	FTE corresponding to the authorised budget 2023	FTE correspondin to the authorised budget 2024
unction Group I	0	1	1	0	1	0	0	0
OTAL	30	29	29	30	27	32	32	32

Seconded National Experts

Seconded National Experts	FTE corresponding to the authorised budget 2020	Executed FTE as of 31/12/2020	Headcount as of 31/12/2020	FTE corresponding to the authorised budget 2021	Executed FTE as of 01/09/2021[50]	FTE corresponding to the authorised budget 2022	FTE corresponding to the authorised budget 2023	FTE correspondin to the authorised budget 2024
OTAL	12	8	8	12	9	12	12	12

Table 3: Recruitment forecasts 2022 following retirement / mobility or new requested posts (indicative table)

JOB TITLE IN THE AGENCY	TYPE OF CONTRACT (OFFICIAL, TA OR CA)		TA/OFFICIAL **Function group/grade of recruitment internal (Brackets) and external (single grade) foreseen for publication ***		CA **Recruitment Function Group (I, II, III and IV)**
	Due to foreseen retirement/ mobility	**New post requested due to additional tasks**	**Internal (brackets)**	**External (brackets)**	
Experts		6 AD posts[51]	n/a	n/a	n/a
Officers		n/a	n/a	n/a	2[52]
Assistant		n/a	n/a	n/a	n/a

[50] In-house SNEs including 01.10.2021. Data of reference 16.09.2021.
[51] The total AD posts includes 3 AD already foreseen and the additional 3 AD new posts.
[52] New 2 CA posts, pending budget approval.

Table 4: Recruitment exercise results from 2021 for TA, CA and manager call

Category		Number of eligible applications			Number of candidates put on a reserve lists			Number of candidates recruited[53]		
Member State	Gender	TA call	CA call	Managers	TA call	CA call	Managers	TA call	CA call	Managers
Austria	Male	6		2						
	Female	1		1						
Belgium	Male	13	2	5	2		1	1		1
	Female	9	4	1						
Bulgaria	Male	11	6	2	1					
	Female	17	5		1					
Croatia	Male	4	3		1					
	Female	2	1	1						
Cyprus	Male	13	6	3						
	Female	7	5	4		1			1	
Czech	Male	6	5	1						
	Female	1		2						
Danish	Male	1								
	Female									
Dutch	Male	7	1	2	1			1		
	Female	2								
Estonian	Male	7	3							
	Female	3								
Finland	Male	3	1	2						
	Female	6								
French	Male	25	8	8	1					
	Female	15	10	2	1			1		
Greece	Male	411	199	90	30	3		3	1	
	Female	254	182	42	9	4	1	2		1
Germany	Male	16	2	4	2	1	1	1		

[53] The numbers include the offers sent and accepted as of 14.06.2021

	Female	5	1	1						
Hungary	Male	5	2	1						
	Female	3	2							
Ireland	Male	7	2							
	Female	2								
Italian	Male	79	35	18	2	3	2		1	1
	Female	36	21	2	3	1			1	
Latvia	Male	5								
	Female	3	4	2			1			1
Lithuanian	Male	3								
	Female	3								
Luxembourg	Male	1	1							
	Female	1								
Maltese	Male	3	1	2						
	Female	1								
Polish	Male	15	9	2		1			1	
	Female	11	7	1	1	1		1		
Portuguese	Male	16	6	2	3		1	1		
	Female	7	1	1	1					
Romanian	Male	24	8	3	3			2		
	Female	24	12	2	1			1		
Spanish	Male	42	13	10	5		1	2		
	Female	19	12	1						
Slovakian	Male	2	2	1						
	Female	3	1							
Swedish	Male	5	2	2						
	Female	1		5						
Slovenian	Male	3	2	1						
	Female	4	3							

V. HUMAN RESOURCES QUALITATIVE

A. Recruitment policy

Implementing rules in place:

		YES	NO	IF NO, WHICH OTHER IMPLEMENTING RULES ARE IN PLACE
Engagement of CA	Model Decision C(2019)3016	x		
Engagement of TA	Model Decision C(2015)1509	x		
Middle management	Model decision C(2018)2542	x		
Type of posts	Model Decision C(2018)8800		x	C(2013) 8979

B. Appraisal and reclassification/promotions

Implementing rules in place:

		YES	NO	IF NO, WHICH OTHER IMPLEMENTING RULES ARE IN PLACE
Reclassification of TA	Model Decision C(2015)9560	x		
Reclassification of CA	Model Decision C(2015)9561	x		

Table 1: **Reclassification of TA/promotion of official**

AVERAGE SENIORITY IN THE GRADE AMONG RECLASSIFIED STAFF							
Grades	**Year 2016**	**Year 2017**	**Year 2018**	**Year 2019**	**Year 2020**	**Actual average over 5 years**	**Average over 5 years** **(According to decision C(2015)9563)**
AD05	-	-	-	-	-	-	2.8
AD06	1	1	2	3	-	3,7	2.8
AD07	1	-	-	-	1	3	2.8
AD08	1	1	1	-	2	6	3
AD09	-	-	1	-	-	10	4
AD10	-	-	-	-	-	-	4
AD11	1	-	-	-	-	3	4
AD12	-	-	-	-	-	-	6.7
AD13	-	-	-	-	-	-	6.7
AST1	-	-	-	-	-	-	3
AST2	-	-	-	-	-	-	3
AST3	1	1	1	-	-	4,42	3
AST4	1	1	1	-	1	5,25	3
AST5	1	-	1	-	-	5,5	4

AST6	1	-	-	-	1	4	4
AST7	-	-	-	-	-	-	4
AST8	-	-	-	-	-	-	4
AST9	-	-	-	-	-	-	N/A
AST10 **(Senior assistant)**	-	-	-	-	-	-	5

There are no AST/SCs at ENISA: n/a

AST/SC1							4
AST/SC2							5
AST/SC3							5.9
AST/SC4							6.7
AST/SC5							8.3

Table 2: Reclassification of contract staff

FUNCTION GROUP	GRADE	STAFF IN ACTIVITY AT 1.01.2019	HOW MANY STAFF MEMBERS WERE RECLASSIFIED IN YEAR 2020	AVERAGE NUMBER OF YEARS IN GRADE OF RECLASSIFIED STAFF MEMBERS	AVERAGE NUMBER OF YEARS IN GRADE OF RECLASSIFIED STAFF MEMBERS ACCORDING TO DECISION C(2015)9561
CA IV	17	1	-	-	Between 6 and 10 years
	16	0	-	-	Between 5 and 7 years
	15	1	-	-	Between 4 and 6 years
	14	9	-	-	Between 3 and 5 years
	13	3	1	3,9	Between 3 and 5 years
CA III	11	1	1	2	Between 6 and 10 years
	10	5	1	3	Between 5 and 7 years
	9	3	1	4,2	Between 4 and 6 years
	8	0	0	-	Between 3 and 5 years
CA II	6	-	-	-	Between 6 and 10 years
	5	-	-	-	Between 5 and 7 years
	4	-	-	-	Between 3 and 5 years
CA I	3	1	-	-	n/a
	2	-	-	-	Between 6 and 10 years
	1	-	-	-	Between 3 and 5 years

C. Gender representation

Table 1: Data on 01.09.2021 statutory staff (only temporary agents and contract agents on 01.09.2021 and accepted offers and resignations up until and including 15.11.2021[54])

		OFFICIAL		TEMPORARY		CONTRACT AGENTS		GRAND TOTAL	
		Staff	%	Staff	%	Staff	%	Staff	%
Female	Administrator level	-	-	18	-	15	-	-	-
	Assistant level (AST & AST/SC)	-	-	11	-	-	-	-	-
	Total	-	-	29	66	15	34	44	44,9
Male	Administrator level	-	-	36	-	12	-	-	-
	Assistant level (AST & AST/SC)	-	-	6	-	-	-	-	-
	Total	-	-	42	77,8	12	22,2	54	55,1
Grand Total		-	-	71	72,5	27	27,5	98	100%

Table 1: Data on 31/12/2020 statutory staff (only, temporary agents and contract agents, including last entry into service on 16/12/2020)

		OFFICIAL		TEMPORARY		CONTRACT AGENTS		GRAND TOTAL	
		Staff	%	Staff	%	Staff	%	Staff	%
Female	Administrator level	-	-	11	-	15	-	-	-
	Assistant level (AST & AST/SC)	-	-	10	-	-	-	-	-
	Total	-	-	21	58	15	42	36	46
Male	Administrator level	-	-	27	-	11	-	-	-
	Assistant level (AST & AST/SC)	-	-	5	-	-	-	-	-
	Total	-	-	32	74	11	26	43	54

[54] Data of reference for the figures 16.09.2021.

Grand Total		-	-	53	67	26	33	79	100%

Table 2: Data regarding gender evolution over 5 years of the Middle and Senior management (01.09.2021 and accepted offers up until and including 16.10.2021)[55]

	2016		01.09.2021	
	Number	%	Number	%
Female Managers	0	0	3	33,3
Male Managers	10	100	6[56]	66,7

The focus of the Agency being cybersecurity hints at the reason for a certain gender imbalance. Nevertheless, an improvement has been noted during the past five years. Continuous efforts to encourage female involvement in this domain have borne fruit, however, further efforts should be envisaged in order to achieve a higher percentage of female middle and senior managers at ENISA in the upcoming years.

D. Geographical Balance

Table 1: Provisional data on 01.09.2021 - statutory staff only (TAs, CAs and accepted offers and resignations up until and including 15.11.2021)[57]

[55] Date of reference for the figures 16.09.2021.
[56] This category comprises Heads of Unit and Team Leaders
[57] Date of reference for the figures 16.09.2021.

NATIONALITY	AD + CA FG IV		AST/SC- AST + CA FGI/CA FGII/CA FGIII		TOTAL	
	Number	**% of total staff members in AD and FG IV categories**	**Number**	**% of total staff members in AST SC/AST and FG I, II and III categories**	**Number**	**% of total staff**
BE	5	6,8	2	8	7	7,1
BG	2	2,74	-	-	2	2
CY	1	1,37	2	8	3	3
CZ	1	1,37	-	-	1	1
DE	2	2,74	-	-	2	2
Double *58	4	5,5	3	12	7	7.1
EE	1	1,37	-	-	1	1
ES	3	4,2	1	4	4	4,1
FR	3	4,2	1	4	4	4,1
GR	26	35,6	12	48	38	38,8
IT	5	6,8	-	-	5	5,1
LT	-	-	1	4	1	1
LV	2	2,74	-	-	2	2
NL	3	4,2	-	-	3	3
PL	3	4,2	1	4	4	4,1
PT	3	4,2	1	4	4	4,1
RO	7	9,6	0	0	7	7,1
SE	2	2,74	-	-	2	2
SK	-	-	1	4	1	1
TOTAL	73	74.5	25	25.5	98	100

[58] Double nationalities comprise staff members who also have non-EU nationalities (i.e. Italian/Australian, Belgian/British, Cypriot/Greek, German/Greek, Dutch/Greek etc.).

Double nationalities comprise staff members who also have non-EU nationalities (i.e. Italian/Australian, Belgian/British, Cypriot/Greek, German/Greek, Dutch/Greek etc.).

Table 2: Evolution over 5 years of the most represented nationality in the Agency

MOST REPRESENTED NATIONALITY	2016		1.9. 2021	
	Number	**%**	**Number**	**%**
Greek	27 (out of 68)	39,7	38 (out of 98)	38,8

Looking back to 2020, it has been noted that the positive mesures to improve the diversity of nationalities which had taken place in 2019 and 2020, have borne fruit. The most represented nationality has seen a decrease of 1% over the past 5 years. This can be attributed to the broad outreach campaigns on popular media across the European Union, closer consideration on the nationality spread in relation to competencies requested, and specific provisions on the vacancy notices have been continued[59].

.E. Local office in Brussels, Belgium

In 2020 ENISA put forward a proposal to open a local office in accordance with CSA Art 20 (5). The number of the staff in each local office shall not exceed 10 % of the total number of ENISA's staff located in the Member State in which the seat of ENISA is located.

The main approval steps were:

- The June 2020 MB gave the ED its prior consent to proceed with the establishment preparations.
- Hellenic (January 2021) and Belgian (August 2020) authorities gave their positive opinion.
- June 2021: COM adopted Decision C(2021) 4626 of 23 June 2021, giving its prior consent.
- July 2021: ENISA MB confirmed the establishment.

Indicative resources foreseen:

Resources (indicative)	**2021**	**2022**	**2023**	**2024**
Head count (FTEs)	**2-3**	**4 -7**	**4-10**	**4-10**
Budget (one-off & maintenance costs)	**25.000**	**500.000**	**170.000**	**170.000**

[59] The seeming imbalance related to the most represented nationality at ENISA is related to several factors, such as, for example, the level of posts and related salaries which may be perceived as less appealing for job seekers in relatively more advanced member state economies; the fact that ENISA has a better position as employer compared to average conditions offered in the Greek job market; the small job market in Greece for cybersecurity professionals; historic decisions taken by previous AIPNs. Another reason that may be cited is the need for stability during the start up phase of the Agency, as staff from the hosting member state (Greece) is less prone to resign (resulting in lesser turnover), which in combination with the relatively young age of the Agency compared to others, still has its original impact; the relatively better academic profile of Greek candidates that bears for lower level posts; the relatively smaller payroll cost for staff that is relatively better qualified than average while costing less if expatriation allowance is considered, as well as the general predisposition to retain a lower level position in the home country.

The practical preperations for the Brussels local office are at an advanced stage.

F. Schooling

Agreement in place with the European School of Heraklion	
Contribution agreements signed with the EC on type I European schools	**No**
Contribution agreements signed with the EC on type II European schools	**Yes**
Number of service contracts in place with international schools:	**For the school year 2021-2022, the process for the financial support for the staff of ENISA in relation to the cost of schooling has been updated via EDD 2021-41, leading to the abolishment of SLAs**

VI. ENVIRONMENT MANAGEMENT

This will depend on the new headquarters building however ENISA is looking into opportunities to strengthen its environmental management as such a new output has been introduced in 2022 to carry out an overarching audit on the CO2 impact of all operations of the Agency and develop and implement a targeted action plan The objective of this undertaking is for the Agency to be climate neutrality by 2030.

VII. BUILDING POLICY

In 2021 ENISA relocated to a new headquarters building in Athens, Greece. The building policy will be developed in the course of 2022.

VIII. PRIVILEGES AND IMMUNITIES

Agency privileges	Privileges granted to staff	
	Protocol of privileges and immunities / diplomatic status	Education / day care
In accordance with Art. 23 of Regulation (EU) No 2019/881 of the European Parliament and of the Council of 17 April 2019, the protocol No 7 on the privileges and immunities of the European Union annexed to the TEU and the TFEU applies to the Agency and its staff. The Greek Government and ENISA signed a Seat Agreement the 13 November 2018, which was ratified by Greek Law 4627/2019 on the 25 September 2019 and entered in to force on the 04 October 2019 and is applicable to ENISA and its staff.	In accordance with Article 35 of Regulation (EU) No 2019/881 of the European Parliament and of the Council of 17 April 2019, the protocol No 7 on the privileges and immunities of the European Union annexed to the TEU and the TFEU applies to the Agency and its staff. The Greek Government and ENISA signed a Seat Agreement the 13 November 2018, which was ratified by Greek Law 4627/2019 on the 25 September 2019 and entered in to force on the 04 October 2019 and is applicable to ENISA and its staff.	A public School of European Education, Type 2, was founded in 2005 by the Greek government in Heraklion – Crete for the children of the staff of ENISA. There is no European School operating in Athens.

IX. EVALUATIONS

External consultant are contracted to carry annual ex-post evaluation of operational activities. The scope of the evaluation focusses on ENISA's operational activities. The overall aim of the annual evaluations is to evaluate the effectiveness, efficiency, and coherence and relevance.

Stakeholders consulted generally agree that the EU Agency for Cybersecurity is the only entity that could possibly achieve such results, is seen as a key enabler of knowledge, experience and expertise and allowing the creation of a strong cybersecurity community. The evaluation also revealed how ENISA is perceived as a strong and credible partner at EU level and the activities seen as pertinent for the Member States. The report therefore concludes on an extremely positive note, acknowledging the added value of ENISA's activities for the whole EU.

The ex ante evaluation included desk research and interviews with key ENISA stakeholders. It concluded that given the restructuring of the Programming Document 2021-2023, the structure of ENISA's SPD would not require any changes, but it was recommended that certain outputs should be strengthened with a specific focus on the following areas:

- a proactive shaping of the political agenda;
- developing a transversal focus on digital strategic autonomy and its implications on cybersecurity;
- reinforcing the cooperative response by an insight-driven approach;
- focusing on stakeholder management, awareness raising and activities targeting industry.

ENISA uses an internal monitoring system that intends to support the project management function, which includes the project delivery and resources allocation. The regular reporting and the ENISA management team uses this information for managerial purposes. Moreover, ENISA have implemented a mid-term review procedure and regular weekly management team meetings. ENISA has undertaken a study to upgrade the use of the electronic tool in the internal project management and overall delivery of the Agency WP.

X. STRATEGY FOR THE ORGANISATIONAL MANAGEMENT AND INTERNAL CONTROL SYSTEMS

The Agency's strategy for an effective internal control is based on best international practices and on the Internal Control Framework (COSO Framework's international Standards).

The Control Environment is the set of standards of conduct, processes and structures that provide the basis for carrying out internal control across ENISA. The Management Team set the tone at the top with respect to the importance of the internal control, including expected standards of conduct.

Risk assessment is the Agency's dynamic and iterative process for identifying and assessing risks which could affect the achievement of objectives, and for determining how such risks should be managed.

The control activities ensure the mitigation of risks related to the achievement of policy, operational and internal control objectives. They are performed at all levels of the organisation, at various stages of business processes, and across the technology environment. They may be preventive or detective and encompass a range of manual and automated activities as well as segregation of duties.

Information is necessary for the organisation to carry out internal control and to support the achievement of objectives. In this aspect it is needed to consider external and internal communication. External communication provides the specific Agency stakeholders and globally the EU citizens with information on ENISA's policy, objectives, actions and achievements. Internal communication provides to ENISA staff with the information required to support the achievement of objectives and the awareness for day-to-day controls.

Continuous and specific assessments are used to ascertain whether each of the five components of internal control is present and functioning. Continuous assessments, built into business processes at different levels of the organisation, provide timely information on any deficiencies. Findings are assessed and deficiencies are communicated and corrected in a timely manner, with serious matters reported as appropriate.

The Common Approach on EU Decentralised Agencies foresees that EU agencies should be more active concerning fraud prevention issues and that the related communication forms an essential part of its success. In order to implement this, the European Anti-Fraud Office (OLAF) recommended that each agency should adopt an anti-fraud strategy that is proportionate to its fraud risks. Rules for the prevention and management of conflicts of interests are part of the anti-fraud strategy of the Agency.

XI. PLAN FOR GRANT, CONTRIBUTION OR SERVICE-LEVEL AGREEMENTS

ENISA does not receive any form of grant.

Table below provides a summary of the SLA and agreements of the agency including contracted amount where necessary:

Title	Type	Contractor	Contracted amount
10th Amendment of SLA with CERT-EU-001-00	SLA	EUROPEAN COMMISSION	€24.480,00
Global SLA with DIGIT	SLA	EUROPEAN COMMISSION	
SLA for Provision of electronic data back up services with BEREC	SLA	OFFICE OF THE BODY OF EUROPEAN REGULATORS FOR ELECTRONIC COMMUNICATIONS (BEREC OFFICE)	
SLA and SDA with DG BUDG Implementation and usage of ABAC System	SLA	EUROPEAN COMMISSION	€46.000,00
SLA for Shared Support Office (SSO)_EUAN	SLA	EUROPEAN FOOD SAFETY AUTHORITY EFSA	€2.828,17
SLA with CEDEFOP	SLA	CEDEFOP	
SLA with DG HR	SLA	EUROPEAN COMMISSION	
SLA with EASA - Permanent Secretariat	SLA	EASA	
SLA with EPSO and EUSA (updated)	SLA	EUROPEAN PERSONNEL SELECTION OFFICE (EPSO)	
SLA with European Administrative School	SLA	EAS	
SLA with Office for Official Publications of the European Communities	SLA	OPOCE Publications Office	
SLA with PMO	SLA	PMO	
Agreement on Strategic Co-operation with EUROPOL	Agreement	EUROPEAN POLICE OFFICE EUROPOL	

Agreement with Hellenic Postal Services A.E. - Athens office	Agreement	ELLINIKA TACHYDROMEIA ELTA AE	50 EUR/month
Agreement with Hellenic Postal Services A.E. - Heraklion office	Agreement	ELLINIKA TACHYDROMEIA ELTA AE	80 EUR/month
Agreement with Translation Centre for the Bodies of the EU	Agreement	CdT	
Austrian signature scheme for e-card and mobile signature_A-Trust	Agreement	A-TRUST GESELLSCHAFT FUR SICHERHEITSSYSTEME IM ELEKTRONISCHEN DATENVERKEHR GMBH	
Collaboration Agreement in the field of standardization	Agreement	CEN & CENELEC	
Cooperation Agreement between ETSI and ENISA	Agreement	European Telecommunications Standards Institute (ETSI)	
Cooperation Plan 2021 – 2023 between EU-LISA and ENISA	Agreement	EU-LISA - EUROPEAN AGENCY	
Joint ENISA - EUROPOL /EC3 WG on Security and Safety Online	Agreement	EUROPEAN POLICE OFFICE EUROPOL	
Lease Agreement Athens office	Agreement	Prodea Investments	
Maintenance Agreement for Franking machines	Agreement	PAPAKOSMAS NTATATECHNIKA EPE	57 EUR/month
Mandate and Service agreement for "Type II European School" with EC	Agreement	DG HR	
Mission Charter of the IAS_REVISED	Agreement	IAS	
Non-Disclosure Agreement CT1607860_Confidential and proprietary document between 12 Parties	Agreement		
Provision of water fountain and water bottles for Athens office	Agreement	EFODIASTIKI KATALANOTIKI AGATHON EPE	6 EUR/pc
Cooperation Agreement with FORTH	Memorandum of Understanding	FORTH	
Cooperation between EDA and ENISA	Memorandum of Understanding	EUROPEAN DEFENCE AGENCY - EDA	
MoU on bilateral cooperation with EUIPO	Memorandum of Understanding	EUIPO	€16.803,58

MoU with Universität der Bundeswehr München	Memorandum of Understanding	Universität der Bundeswehr München (UniBw M)	
Structured cooperation between ENISA and CERT EU	Memorandum of Understanding	CERT-EU	
Working Arrangement Agreement with eu-LISA	Memorandum of Understanding	EU-LISA - EUROPEAN AGENCY	

XII. STRATEGY FOR COOPERATION WITH THIRD COUNTRIES AND/OR INTERNATIONAL ORGANISATIONS

The international strategy foresees a continuation of the strong focus on the EU and EU actors, while also allowing increased flexibility to engage with international partners in line with the strategic objectives outlined in the ENISA Strategy for a Trusted and Cyber Secure Europe of July 2020. The Agency's international strategy is annexed to the Single Programming Document 2022-2024 as a separate document.

XIII. ANNUAL COOPERATION PLAN 2022

The 2022 Annual Cooperation Plan between ENISA, the EU Agency for Cybersecurity, and CERT-EU, the CERT of the EU institutions, bodies and agencies is annexed to the Single Programming Document 2022-2024 as a separate document.

XX-00-00-000-XX-X

ABOUT ENISA

The European Union Agency for Cybersecurity (ENISA) has been working to make Europe cyber secure since 2004. ENISA works with the EU, its member states, the private sector and Europe's citizens to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. Since 2019, it has been drawing up cybersecurity certification schemes. More information about ENISA and its work can be found at www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14, Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN 000-00-0000-000-0
doi: 0000.0000/000000

European Union Agency
for Cybersecurity

Agamemnonos 14
Chalandri 15231 | Attiki | Greece
Tel: +30 28 14 40 9711
E-mail: info@enisa.europa.eu
www.enisa.europa.eu

ADOPTED SPD22-24 ANNEX XII: INTERNATIONAL STRATEGY OF THE EU AGENCY FOR CYBERSECURITY

1. INTRODUCTION

1.1. Article 12 of the Cybersecurity Act (CSA) foresees that "ENISA shall contribute to the Union's efforts to cooperate with third countries and international organisations as well as within relevant international cooperation frameworks to promote international cooperation on issues related to cybersecurity" by different ways, including by facilitating the exchange of best practices and by providing expertise, at the request of the Commission.

1.2. Article 42 of the CSA requires the Management Board of ENISA to adopt "a strategy for relations with third countries and international organisations concerning matters for which ENISA is competent[1]." CSA also refers to specific international organisations (such as OECD, OSCE and NATO) with which ENISA is called to develop relations with (see recital 43).

1.3. Since the entry into force of the CSA, ENISA's exposure to partners outside of the EU has increased both quantitatively and qualitatively[2]. ENISA is also often approached by third countries directly with high expectations of mutual collaboration, and is confronted each time on how best to react. Such welcomed developments call for a more strategic approach to the international dimension of ENISA's work in order to guide the engagement of the Agency with third country partners, as well to direct Agency's response to third country partners seeking cooperation with ENISA.

1.4. This international strategy covers the cooperation with international organisations and with non-EU countries. However, for those non-EU countries or regions with which the EU has special agreements this international strategy should be read in the light of such agreements, looking at where a closer cooperation in the area of cybersecurity is foreseen.

2. ENISA'S OVERALL INTERNATIONAL APPROACH[3]

The mandate of the Agency is to achieve: "a high common level of cybersecurity across the Union, including by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity." Under this mandate, ENISA's strategic aim is to build a trusted and cyber-secure Europe. ENISA's international

[1] Chapter II of Title II the CSA covers all tasks of ENISA and thus outlines areas for which ENISA is competent.

[2] The expectations from various actors inside the EU institutions and from Member States for the Agency to engage more actively internationally have increased, as was stressed in the bilateral interviews undertaken by ENISA in spring 2021. This was also confirmed in the internal survey that ENISA undertook in early 2021.

[3] The directions and provisions in this strategy will not in any way limit or hamper the provisions laid out by Article 12 of CSA.

strategy must therefore be at the service of the Union, advance the achievement of the Agency's mandate within the Union and contribute to its strategy[4].

This underlying premise directs the Agency to be **selective in engaging with international partners** and to limit its overall approach in international cooperation only to those areas and activities, which will have high and measurable added-value towards achieving the Agency's strategic objectives.

International cooperation should be resourced prudently and proportionally. This strategy outlines three approaches that the Agency can use in terms of level of commitment of resources, namely: the *limited*, *assisting* and *outreach* approach.

2.1 LIMITED APPROACH

ENISA's default international approach is 'LIMITED'. Under this ENISA will, in line with its objectives enshrined in Article 4 of CSA, exchange information on an *ad hoc* basis and when needed with relevant international partners[5], to strengthen and develop its expertise and anticipate changes prompted by global developments in cybersecurity. It will seek to promote the Union's values, to advance its strategic objectives and cybersecurity policies when engaging with international partners in meetings, conferences and seminars. Under this approach, ENISA will not commit dedicated resources to pursue this approach, beyond mission or conference costs.

2.2 ASSISTING APPROACH

In line with its mandate to: "actively support Member States, Union institutions, bodies, offices and agencies in improving cybersecurity" (CSA Art. 3(1)), ENISA may respond to requests of assistance, when the request is deemed to add high value to a specific strategic objective and is in line with the Union's policies, namely with third countries and international organisations with whom the Union has agreements or frameworks which promote specific or general cooperation in cybersecurity. Under this '**ASSISTING**' approach, ENISA may exchange and share expertise, contribute in organising trainings and exercises, support the Commission / EU in building and maintain cybersecurity dialogues or support individual cybersecurity activities with international partners organised by the requester. To respond to such requests, ENISA might use resources dedicated to specific strategic objectives under its Single Programming Document (SPD).

2.3 OUTREACH APPROACH

ENISA may follow an '**OUTREACH**' approach for specific aims and provisions of the strategic objectives outlined further in this strategy, to proactively engage with specific international partners to be able to advance the Agency's strategic objectives and fulfil the objectives of the CSA. Under this approach, ENISA may plan dedicated resources under its SPD in pursuit of this approach.

3. PRINCIPLES GOVERNING ENISA'S INTERNATIONAL APPROACH

1. ENISA will focus its international cooperation on partners with whom the Union has strategic economic relationships and who share the Union's values.

2. When cooperation in cybersecurity between the Union and an international partner is explicitly stated in an agreement, ENISA may follow an *outreach* approach, respecting the limits of the agreement provisions.

3. Beyond specific provisions outlined under point 4, ENISA can, when relevant, pursue an *outreach* approach across all of its strategic objectives with the countries belonging to the European Economic Area.

[4] ENISA Strategy - A Trusted and Cyber Secure Europe, available at https://www.enisa.europa.eu/publications/corporate-documents/enisa-strategy-a-trusted-and-cyber-secure-europe
[5] For principles which govern selecting and engaging with international partners, please see point 3

4. ENISA will refrain from engaging with international actors, if contacts with such actors or cooperation with them would be deemed to be incompatible with the Union's interest or with the Union's policy goals.

5. The Agency's International cooperation activities should align and add value to the partnerships of the Member States.

6. When responding to requests under the *assisting* approach not explicitly covered in this Strategy, and also where otherwise appropriate, ENISA will consult and coordinate with the EEAS and the Commission, to ensure that the Agency's international engagement is in line with the Union's policy goals. ENISA will notify the Executive Board of requests under an *assisting* approach and under an *outreach* approach. ENISA will furthermore ensure that its *outreach* activities are in line with the Union's policies by regularly consulting with DG CNECT.

7. In the SPD, ENISA would proportionally evaluate the resources needed for the involvement in any international activities with an *assisting* or *outreach* approach.

8. ENISA will seek prior endorsement of the Executive Board before developing cooperation frameworks or agreements with international organisations and third countries. When such agreements place financial or legal obligations to the Agency, they have to be approved by the Management Board.

9. Within its Annual Activity Report, ENISA will outline all international activities it has pursued under different approaches. In particular it will evaluate and provide assessment of the added value of international activities under an *assisting* or *outreach* approach in pursuit of its strategic objectives.

10. The Agency should be able to react in an agile manner while adhering to these principles.

4. SPECIFIC AIMS AND PROVISIONS UNDER INDIVIDUAL STRATEGIC OBJECTIVES

4.1 STRATEGIC OBJECTIVE "EMPOWERED & ENGAGED COMMUNITIES ACROSS THE CYBERSECURITY ECOSYSTEM"

ENISA exchanges best practices, expertise and promotes international activities to enhance the cybersecurity awareness and education of the various communities of the Union. Furthermore, ENISA can:

- By using the *assisting* approach, give support in terms of expertise to the Western Balkans as a region and/or singular countries and countries belonging to the European Eastern Partnership as a region and/or singular countries;

- By using the *outreach* approach, and by the endorsement of the Management Board, cooperate with third countries with whom there are specific EU agreements to enhance mutual cybersecurity awareness and education in line with the respective specific provisions in such agreements.

4.2 STRATEGIC OBJECTIVE "CYBERSECURITY AS AN INTEGRAL PART OF EU POLICES"

ENISA collects and exchanges information on best practices in cybersecurity policy development and implementation internationally and promotes the projection of EU cybersecurity policies to the benefit of the Union. ENISA's connections with international organisations working on digital security can both contribute to the promotion of EU acquis in this field and feed into EU cybersecurity policy development. Furthermore, ENISA can:

- By using the *assisting* approach, support the relevant Union representatives at the international organisations and regulatory forums with expertise on cybersecurity policies and cybersecurity aspects of Union legislation as outlined under Article 5 of the CSA;

- By using the *assisting* approach provide expertise on cybersecurity policy implementation to the Western Balkans and Eastern Partnership countries;

- By using the *outreach* approach cooperate with the OECD (and like-minded countries such as the US) on mapping and promoting best practices in integrating cybersecurity into different policy domains.

4.3 STRATEGIC OBJECTIVE "EFFECTIVE COOPERATION AMONGST OPERATIONAL ACTORS WITHIN THE UNION IN CASE OF MASSIVE CYBER INCIDENTS"

ENISA's international cooperation should assist and contribute to the Union's incident response and crisis management, in particular by building a trusted network of like-minded international partners – including major global cybersecurity companies and vendors to contribute to Union's common situational awareness and preparedness. Furthermore, ENISA can in line with recital 43 of the CSA and by using the *outreach* approach, contribute to the cooperation with international partners such as OSCE and NATO on joint incident response coordination6.

4.4 STRATEGIC OBJECTIVE "CUTTING-EDGE COMPETENCES AND CAPABILITIES IN CYBERSECURITY ACROSS THE UNION"

ENISA will seek to reach out to international partners to exchange information and best practices in order to enhance and develop cybersecurity competences and capabilities within the Union. Where appropriate, it can participate as an observer in the organisation of international cybersecurity exercises in line with Article 12 of CSA. Furthermore, ENISA can:

- By using the *assisting* approach, contribute into building competences and capabilities in the Western Balkans as a region and/or singular countries by supporting trainings and exercises;

- By using the *assisting* approach, support with relevant expertise the countries belonging to the Eastern Partnership as a region and/or singular countries or countries benefiting from the Union's development programmes;

- In line with recital 43 of the CSA and by using the *assisting* approach, contribute to the organisation of joint cybersecurity exercises with the OECD, the OSCE and NATO.

- Under the *outreach* approach, organise International Cybersecurity Challenges to promote and enhance the competitiveness of the cybersecurity competences in the Union.

- By using the *outreach* approach, and by the endorsement of the Management Board, cooperate with third countries with whom there are specific EU agreements to build and enhance mutual cybersecurity capacities in line with the respective specific provisions in such agreements.

4.5 STRATEGIC OBJECTIVE "A HIGH LEVEL OF TRUST IN SECURE DIGITAL SOLUTIONS"

Without prejudice to possible tasks stemming from Article 12(d) of the CSA, ENISA will seek to advance its expertise and monitor international developments in cybersecurity certification and related standardisation areas, also in line with Article 54 CSA[7]. It will engage with international actors on the supply and demand sides of the cybersecurity market to promote and advance European digital autonomy. Furthermore, ENISA will:

[6] Those activities are to be carried out in full respect of the principles of inclusiveness, reciprocity and the decision-making autonomy of the Union, without prejudice to the specific character of the security and defence policy of any Member State.

[7] Article 54 (Elements of European cybersecurity certification schemes) CSA states that "A European cybersecurity certification scheme shall include at least the following elements: […] (c) references to the international, European or national standards applied in the evaluation or, where such standards are not available or appropriate, to technical specifications that meet the requirements set out in Annex II to Regulation (EU) No 1025/2012 or, if such specifications are not available, to technical specifications or other cybersecurity requirements defined in the European cybersecurity certification scheme; […] (o) the identification of national or international cybersecurity certification schemes covering the same type or categories of ICT products, ICT services and ICT processes, security requirements, evaluation criteria and methods, and assurance levels".

- By using the *outreach* approach, engage with the relevant key strategic economic partners of the Union to promote the EU's cybersecurity certification schemes or candidate schemes;

- By using the *outreach* approach, and in line with recital 23 of the CSA, support the global development and maintenance of standards which underpin the public core of the open internet and the stability and security of its functioning.

4.6 STRATEGIC OBJECTIVE "FORESIGHT ON EMERGING AND FUTURE CYBERSECURITY CHALLENGES"

ENISA aims to exchange information on an ad hoc basis and participate in international fora to raise its expertise on international developments, map global cybersecurity threats as well as research areas and innovation trends which could address emerging challenges.

4.7 STRATEGIC OBJECTIVE "EFFICIENT AND EFFECTIVE CYBERSECURITY INFORMATION AND KNOWLEDGE MANAGEMENT FOR EUROPE"

ENISA aims to gain a better overview and understanding of the international cybersecurity landscape and ensure that relevant cybersecurity information and knowledge which is generated internationally is shared and expanded within the EU cybersecurity ecosystem. ENISA will focus its *outreach* to partners deemed as like-minded (e.g. Japan). Furthermore, ENISA will:

- By using the *outreach* approach, cooperate with OECD and NATO in exchanging expertise for the development of cybersecurity indexes and benchmarks;

- By using the *outreach* approach, and by the endorsement of the Management Board, cooperate with third countries with whom there are specific EU agreements to enhance mutual knowledge and information in line with the respective specific provisions in such agreements..

Athens, November 2021

ANNEX 1

Annual Cooperation Programme with CERT-EU for 2022

(not publically available)

Adopted Statement of Estimates 2022 (Budget 2022)

European Union Agency for Cybersecurity

CONTENTS

1. GENERAL INTRODUCTION

Explanatory statement

Legal Basis:

1. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity)

Reference acts

1. Impact assesment submitted by the Commission on 13 September 2017, on ENISA, the 'EU Cybersecurity Agency', as part of the draft 'Cybersecurity Act' (COM(2017) 477 final)
2. ENISA Financial Rules adopted by the Management Board on 15 October 2019

2. JUSTIFICATION OF MAIN HEADINGS

2.1 Revenue in 2022

The 2021 total revenue amounts to € 24207625 and consists of a subsidy of € 23633000 from the General Budget of the European Union, EFTA countries' contributions € 574625 and a subsidy from the Greek Government for the rent of the offices of ENISA in Greece € 0

€ 610000 might be received further to approval of NIS2 Directive

2.2 Expenditure in 2022

The total forecasted expenditure is in balance with the total forecasted revenue.

Total expenditure under Title 1 amounts to **€12.494.335,00**

Title 2 - Buildings, equipment and miscellaneous operating expenditure

Total expenditure under Title 2 amounts to **€2.824.300,00**

Title 3 - Operational expenditure

Operational expenditure is mainly related to the implementation of Work Programme 2022 and amounts to **€8.888.990,00**

Title 1 - Staff

The estimate of Title 1 costs is based on the Establishment Plan for 2021, which contains 76 Temporary Agent posts.

3. STATEMENT OF REVENUE 2022

Title Heading Voted Appropriations 2019 in € Voted Appropriations - Amending Budget 1/2020 in € Voted Appropriations 2021 € Draft Proposed Appropriations 2022 €

633.000

0

0 Remarks - budget 2022

1EUROPEAN COMMUNITIES SUBSIDY15.910.00020.646.00022.248.000Total subsidy of the European Communities **2THIRD COUNTRIES** 24.207.625

CONTRIBUTION382.952503.120585.060 Contributions from Third Countries. **3OTHER CONTRIBUTIONS640.000435.844640.000**Subsidy from the Government of Greece

4ADMINISTRATIVE OPERATIONS097.9200 Other expected income.

GRAND TOTAL16.932.95221.682.88423.473.060 Draft Proposed Appropriations 2022 €

Voted Appropriations -

ArticleVoted Appropriations 2019 Voted Appropriations

HeadingAmending Budget Remarks - budget 2022

Itemin € 2021 €

1/2020 in €

23.023.000

610.000

23.633.000

1EUROPEAN COMMUNITIES SUBSIDY

10EUROPEAN COMMUNITIES SUBSIDY 633.000

Regulation (EU) N° 526/2013 establishing an European Union Agency for Network and

574.625

100European Communities subsidy*15.910.00020.646.00022.248.000 *100European Communities subsidy - NIS Reserve*n/an/an/aConditional to approval of NIS2 Directive* 574.625

574.625

Information Security.

CHAPTER 1015.910.00020.646.00022.248.000

TITLE 115.910.00020.646.00022.248.000 0

2THIRD COUNTRIES CONTRIBUTION 0

20THIRD COUNTRIES CONTRIBUTION

***200Third Countries contribution*382.952503.120585.060**Contributions from Associated Countries. **CHAPTER 2 0382.952503.120585.060**

0

TITLE 2382.952503.120585.060 0

3	**OTHER CONTRIBUTIONS**						0
30	**OTHER CONTRIBUTIONS**						24.207.625
300	***Subsidy from the Ministry of Transports of Greece***		**640.000**	**435.844**	**640.000**Subsidy from the		Government of Greece.
		CHAPTER 30	**640.000**	**435.844**	**640.000**		
		TITLE 3	**640.000**	**435.844**	**640.000**	Draft Proposed Appropriations 2022 €	
4	**ADMINISTRATIVE OPERATIONS**						
40	**ADMINISTRATIVE OPERATIONS**						
400	***Administrative Operations***		0	97.920	0Revenue from	**12.494.335**	administrative operations.
		CHAPTER 40	**0**	**97.920**	**0**	**2.824.300**	

TITLE 4 0 97.920 0 GRAND TOTAL 8.888.990

16.932.952 21.682.884 23.473.060 24.207.625

4. STATEMENT OF EXPENDITURE 2022

Voted Appropriations -

Voted Appropriations 2019 Voted Appropriations

Title	Heading	Amending Budget 1/2020 in €	Remarks - budget 2022 in €	2021 €	
1	STAFF	9.387.948	11.203.334	10.775.409	Total funding for covering personnel costs.
2	BUILDINGS, EQUIPMENT AND MISCELLANEOUS OPERATING EXPENDITURE	2.677.000	3.150.568	3.547.651	Total funding for covering general administrative costs.
3	OPERATIONAL EXPENDITURE	4.868.004	7.328.981	9.150.000	
	GRAND TOTAL	16.932.952	21.682.884	23.473.060	

1 STAFF

11 STAFF IN ACTIVE EMPLOYMENT

110 Staff holding a post provided for in the establishment plan

Total funding for operational expenditures. 1100 Basic salaries 5.000.000 5.484.400 6.453.819

Staff Regulations applicable to officials of the European Communities and in particular Articles 62 and 66 thereof. This appropriation is intended to cover salaries, allowances and employee contributions on salaries of permanent officials and Temporary Agents (TA).

1100 NIS reserve basic salaries n/a n/a n/aConditional to *approval of NIS2 Directive - 3 TAs*

Article 1 1 0 5.000.000 5.484.400 6.453.819 7.911.489

111 Other staff

450.000 Conditions of employment of other servants of the European Communities and in

8.361.489 particular

1110 Contract Agents 1.650.000 1.476.000 2.106.500Article 3 and Title III thereof. This appropriation is intended to cover salaries, allowances and

employee contributions on salaries of Contract Agents (CA).

1110 NIS reserve contract agents n/a n/a n/aConditional to 1.659.391 *approval of NIS2 Directive - 2 CAs*

1113 Seconded National Experts (SNEs) 144.000 165.684 250.000This appropriation is intended to cover basic salaries and all benefits of SNEs. Article 1 1 1

1.794.000 1.641.684 2.356.500 *160.000*

CHAPTER 11 6.794.000 7.126.084 8.810.319 657.000

12 RECRUITMENT/DEPARTURE EXPENDITURE 2.476.391

120 Expenditure related to recruitment **10.837.880**

This appropriation is intended to cover expenditure related to recruitment, e.g. incurred for

1200 Expenditure related to recruitment 97.000 275.308 49.087interviewing

10.000 candidates, external selection committee members, screening applications and other

related costs.

10.000

Article 1 2 0 97.000 275.308 49.087

121 Expenditure on entering/leaving and transfer

17.000 Staff Regulations applicable to officials of the European Communities and in particular

1210 Expenses on Taking Up Duty and on End of Contract 40.000 48.201 32.000Articles 20 and 71 thereof and Article 7 of Annex VII thereto. This appropriation is intended

to cover the travel expenses of staff (including members of their families).

204.000 Staff Regulations applicable to officials of the European Communities and in particular

1211 Installation, Resettlement and Transfer Allowance 356.042 137.424 145.000Articles 5 and 6 of Annex VII thereto. This appropriation is intended to cover the installation

allowances for staff obliged to change residence after taking up their duty.

89.000 Staff Regulations applicable to officials of the European Communities and in particular

1212 Removal Expenses 247.000 111.462 72.000Articles 20 and 71 thereof and Article 9 of Annex VII thereto. This appropriation is intended

to cover the removal costs of staff obliged to change residence after taking up duty.

92.000 Staff Regulations applicable to officials of the European Communities and in particular

Articles 20 and 71 thereof and Article 10 of Annex VII thereto, as well as Articles 25 and 67 of

402.000

1213 Daily Subsistence Allowance 228.906 132.291 112.000

412.000

the Conditions of Employment of other Servants. This appropriation is to cover the costs of daily subsistance allowances.

Article 1 2 1 871.948 429.378 361.000 **CHAPTER 1 2 968.948 704.686 410.087**

13 SOCIO-MEDICAL SERVICES AND TRAINING

131 Medical Service

1310 Medical Service 75.000 45.310 53.882 This appropriation is intended to cover the costs of annual medical visits and inspections, occupational doctor services as well as pre-recruitment medical costs and other costs related to medical services.

Aticle 1 3 1 75.000 45.310 53.882

132 Training

This appropriation is intended to cover the costs of language and other training needs as well

1320 Language Courses

63.000 and Other Training

250.000

63.000 330.428

280.182 as

teambuilding activities.

Article 1 3 2 250.000 330.428 280.182 220.000

133 Social welfare

This appropriation is intended to cover other welfare expenditure such as health related 1330 Other welfare expenditure n/a n/a 220.000 250.000activities to promote well-being of staff, other activities related to

internal events, other

40.000 welfare measures.

This appropriation is intended to cover the subsidy for the functioning of the School of

1331 Schooling & Education expenditure n/a n/a 500.000European

530.000 Education of Heraklion and other expenditure relevant to schooling & education of children of the Agency staff.

Article 1 3 3 0 0 750.000 570.000

CHAPTER 1 3 325.000 375.738 1.084.064 853.000

14 TEMPORARY ASSISTANCE

140 European Commission Management Costs

70.000

1400 EC Management Costs 58.000 39.149 70.939This appropriation is intended to cover the EC management costs.

70.000

Article 1 4 0 58.000 39.149 70.939

141 Social welfare

n/a *As from 2021, whereas the budget structure has been aligned with the SPD, this budget line*

n/a

1411 Other welfare expenditure 110.000 172.537 n/a *has been moved to budget line 1330*

0 *As from 2021, whereas the budget structure has been aligned with the SPD, this budget line*

1412 Schooling & Education expenditure 420.000 470.000 n/a *has been moved to budget line 1331*

Article 1 4 1 530.000 642.536 0 321.455

142 Temporary Assistance

n/a This appropriation is intended to cover the costs of temporary assistance (trainees and

1420 Interim Service 572.000 1.673.006 400.000 interim services).

n/a

As from 2021, whereas the budget structure has been aligned with the SPD, this budget line

1421 Consultants 115.000 625.135 n/a *has been moved to budget line 2220* 321.455

391.455

12.494.335

As from 2021, whereas the budget structure has been aligned with the SPD, this budget line

1422 Internal Control and Audit 25.000 17.000 n/a *has been moved to budget line 2220*

Article 1 4 2 712.000 2.315.141 400.000

CHAPTER 1 4 1.300.000 2.996.826 470.939

Total Title 1 9.387.948 11.203.334 10.775.409

78.151

2 BUILDINGS, EQUIPMENT AND MISCELLANEOUS OPERATING EXPENDITURE

n/a

20 BUILDINGS AND ASSOCIATED COSTS

145.317

200 Buildings and associated costs

250.083 This appropriation is intended to cover the payment of rent for buildings or parts of buildings

40.000

2000 Rent of buildings 640.000 435.844 640.000

occupied by the Agency and the hiring of parking
spaces.

As from 2021, whereas the budget structure has been aligned with the SPD, this budget line

2002 Building Insurance 6.000 4.500 n/a *has been moved to budget line 2003*

This appropriation is intended to cover the costs of utitlities and insurance of the premises of

2003 Water, gas, electricity, heating and insurance 130.000 58.500 76.050 the Agency.

This appropriation is intended to cover the costs of cleaning and upkeeping of the premises

2004 Cleaning and maintenance 74.000 100.120 120.000

used by the Agency.

2005 Fixtures and Fittings 25.000 25.650 50.000

This appropriation is intended to cover the fitting-out of the premises and repairs in the building.

2006 Security equipment 25.000 64.651 n/a

As from 2021, whereas the budget structure has been aligned with the SPD, this budget line has been moved to budget line 2007

This appropriation is intended to cover expenditure on buildings connected with security and

2007 Security Services and Equipment 140.000 134.084 140.000safety, in particular contracts governing building surveillance as well as n/a purchases and

maintenance cost of equipment related to security and safety of the building and the staff.

157.590

The appropriation is intended to cover expenditure on buildings not specially provided for in

2008 Other expenditure on buildings 60.000 106.470 378.558the articles in Chapter 20, for example market survey costs for rent of buildings, costs of moving to
and/or establishing new premises of the Agency and other handling costs. 243.409

Article 2 0 0 1.100.000 929.820 1.404.608 **CHAPTER 2 0**

1.100.000 929.820 1.404.608 914.550

914.550

21 MOVABLE PROPERTY AND ASSOCIATED COSTS

210 Technical Equipment and installations

10.000 This appropriation is intended to cover expenditure of acquiring technical equipment, as

10.000 well

2100 Technical Equipment and services

125.000 25.000 10.968 30.000 as

maintenance and services related to it.

Article 2 1 0 25.000 10.968 30.000 125.000

211 Furniture

10.000 This appropriation is intended to cover the costs of purchasing, leasing, and repairs of

10.000

15.000

15.000

160.000

27.000

22.000

n/a

49.000

1.000

1.000

270.000

270.000

320.000

n/a

n/a

n/a

0

1.065.000

364.750

1.429.750

1.429.750

2.824.300

2110	Furniture	15.000	16.303	49.000	furniture.
	Article 2 1 1	15.000	16.303	49.000	
212	***Transport Equipment***				
2121	Maintenance and Repairs of transport equipment	12.000	9.000	10.000	This appropriation is intended to cover the costs of maintenance and repairs of transport equipment as well as insurance and fuel.
	Article 2 1 2	12.000	9.000	10.000	
213	***Library and Press***				
2130	Books, Newspapers and Periodicals	6.000	17.803	10.000	This appropriation is intended to cover the purchase of publications and subscriptions to information services necessary for the work of the Agency, including books and other publications, newspapers, periodicals, official journals and subscriptions.
	Article 2 1 3	6.000	17.803	10.000	
	CHAPTER 2 1	**58.000**	**54.074**	**99.000**	
22	**CURRENT CORPORATE EXPENDITURE**				
220	***Stationery, postal and telecomunications***				
2200	Stationery and other office supplies	60.000	52.233	30.000	This appropriation is intended to cover the costs of office stationery and the purchase of office kitchen consumables.
2201	Postage and delivery charges	20.000	30.000	20.000	This appropriation is intented to cover post office and special courrier costs.
2203	Other Office Supplies	23.000	15.469	n/a	*As from 2021, whereas the budget structure has been aligned with the SPD, this budget line has been moved to budget line 2200*
	Article 2 2 0	103.000	97.702	50.000	
221	***Financial charges***				
2210	Bank charges and interest paid	1.000	1.000	1.000	This appropriation is intended to cover bank charges, interest paid and other financial and banking costs.
	Article 2 2 1	1.000	1.000	1.000	
222	***Outsourcing consultancy services for corporate activities***				
2220	Outsourcing consultancy services for corporate activities	n/a	n/a	747.696	This appropriation is intended to cover expenditure of contracting consultants linked to administrative support services and horizontal tasks, e.g. in HR area, IT area, financial, accounting, internal controls, legal consultancy, advisory, audit, external evaluation, strategic consultancy and/or other administrative support services provided by third parties.
	Article 2 2 2	0	0	747.696	

	CHAPTER 2 2	**104.000**	**98.702**	**798.696**	
23	**ICT**				
230	***ICT***				*As from 2021, whereas the budget structure has been aligned with the SPD, these budget lines have been moved to Article 231 Corporate ICT expenditure*
2304	Service Transition	600.000	741.135	n/a	
2305	Service Operations	220.000	184.018	n/a	This appropriation is intended to cover recurrent corporate ICT costs on hardware, software, services and maintenance as well as ENISA website and portals support. This appropriation is intended to cover new investments on corporate ICT as well as one-off projects for hardware, software, services and maintenance as well as ENISA website and portals support.
2307	Service External	595.000	1.142.819	n/a	
	Article 2 3 0	1.415.000	2.067.972	0	
231	***Corporate ICT expenditure***				
2310	Corporate ICT recurrent costs	n/a	n/a	585.347	
2311	Corporate ICT new investments and one-off projects	n/a	n/a	660.000	
	Article 2 3 1		0	1.245.347	
	CHAPTER 2 3	**1.415.000**	**2.067.972**	**1.245.347**	
	Total Title 2	**2.677.000**	**3.150.568**	**3.547.651**	

3	**OPERATIONAL EXPENDITURE**					
30	**ACTIVITIES RELATED TO OUTREACH AND MEETINGS**					
300	***Outreach, meetings and representation expenses***				387.000	
3001	Outreach, meetings, translations and representation expenses	120.000	69.198	650.000	387.000	This appropriation is intended to cover costs of outreach activities (communications, stakeholders' management, publication and translations), meetings (including meetings of ENISA's statutory bodies i.e. MB, AG, NLOs, and meetings with other stakeholders) and other representation costs. It also covers mission costs related to the implementation of Activities 10-11 as defined in the SPD 2021-2023 mainly covering horizontal tasks and other administrative services.
	Article 3 0 0	120.000	69.198	650.000	n/a n/a	
301	*Mission and Representation Costs*				0	
3011	Entertainment and Representation expenses	15.394	5.000	n/a		
3016	Missions	897.930	550.767	n/a	n/a	
	Article 3 0 1	913.324	555.767	0	0 **387.000**	
302	*Other meetings*					
3021	Other Operational meetings	10.000	4.000	n/a	n/a	
	Article 3 0 2	10.000	4.000	0	0	
	CHAPTER 3 0	**1.043.324**	**628.966**	**650.000**	n/a n/a	
32	HORIZONTAL OPERATIONAL ACTIVITIES				n/a	
320	*Conferences and Joint Events*				0	
3200	Horizontal Operational meetings	214.608	65.448	n/a	n/a	
	Article 3 2 0	214.608	65.448	0	0	
321	*Communication and Information dissemination*				n/a	
3210	Communication activities	150.000	205.763	n/a	0	
3211	Internal Communication	0	45.000	n/a	n/a	
3212	Stakeholders' communication	113.000	291.358	n/a	n/a	
	Article 3 2 1	263.000	542.121	0	0 **0**	
323	*Translation and interpretation services*					
3230	Translations	30.072	120.000	n/a		
	Article 3 2 3	30.072	120.000	0		
325	*Operational Systems*					
3250	Operational Systems including website development	57.000	146.079	n/a		

		Article 3 2 5	57.000	146.079	0
326	***Strategy and Evaluation***				
3260	Strategic consultancy		50.000	251.215	n/a
3261	External Evaluations		0	393.100	n/a
		Article 3 2 6	50.000	644.315	0
		CHAPTER 3 2	**614.680**	**1.517.962**	**0**

As from 2021, whereas the budget structure has been aligned with the SPD, these budget lines have been moved to budget line 3001

As from 2021, whereas the budget structure has been aligned with the SPD, this budget line has been moved to budget line 3001

As from 2021, whereas the budget structure has been aligned with the SPD, this budget line has been moved to budget line 3001

As from 2021, whereas the budget structure has been aligned with the SPD, these budget lines have been moved to budget line 3001

As from 2021, whereas the budget structure has been aligned with the SPD, this budget line has been moved to budget line 3001

As from 2021, whereas the budget structure has been aligned with the SPD, this budget line has been moved to Article 231 Corporate ICT expenditure

As from 2021, whereas the budget structure has been aligned with the SPD, these budget lines have been moved to budget line 2220

36	CORE OPERATIONAL ACTIVITIES						
363	*Activity: Expertise*					n/a	
3630	Activity: Expertise		875.000	1.282.536	n/a	0	
		Article 3 6 3	875.000	1.282.536	0		
364	*Activity: Policy*					n/a	
3640	Activity: Policy		1.150.000	1.742.210	n/a	0	
		Article 3 6 4	1.150.000	1.742.210	0		
						n/a	*As from 2021, whereas the budget structure has been aligned with the SPD, these*
						0	*budget*
365							***Activity: Capacity** lines have*
						n/a	*been moved to Chapter 37*
3650	Activity: Capacity		535.000	798.982	n/a	0	
		Article 3 6 5	535.000	798.982	0	**0**	
366	*Activity: Community*						
3660	Activity: Community		650.000	1.358.326	n/a		
		Article 3 6 6	650.000	1.358.326	0	363.000	
		CHAPTER 3 6	**3.210.000**	**5.182.053**	**0**		
37	**CORE OPERATIONAL ACTIVITIES**					363.000	
371	***Activity 1 - Providing assistance on policy development***						
						798.475	This appropriation is intended to cover direct operational costs relevant to the Activity 1
3710	Activity 1 - Providing assistance on policy development		n/a	n/a	280.000	798.475	
							(including operational ICT and mission costs).
		Article 3 7 1	0	0	280.000		
						1.921.265	
372	***Activity 2 - Supporting implementation of Union policy and law***						
						1.921.265	This appropriation is intended to cover direct operational costs relevant to the Activity 2
3720	Activity 2 - Supporting implementation of Union policy and law		n/a	n/a	985.000		
						1.703.350	(including operational ICT and mission costs).
		Article 3 7 2	0	0	985.000		
373	***Activity 3 - Capacity building***					1.703.350	
							This appropriation is intended to cover direct operational costs relevant to the Activity 3
3730	Activity 3 - Capacity building		n/a	n/a	1.400.000		
						824.500	(including operational ICT and mission costs).
		Article 3 7 3	0	0	1.400.000	824.500	
374	***Activity 4 - Enabling operational cooperation***						
							This appropriation is intended to cover direct operational costs relevant to the Activity 4
3740	Activity 4 - Enabling operational cooperation		n/a	n/a	1.110.000		
						1.025.750	(including operational ICT and mission costs).
		Article 3 7 4	0	0	1.110.000	1.025.750	
	Activity 5 - Contribute to cooperative response at Union and Member States level						
375							
	Activity 5 - Contribute to cooperative response at Union and Member This appropriation is intended to cover direct operational costs relevant to the					373.800	Activity 5
3750			n/a	n/a	1.200.000		
	States level (including operational ICT and mission costs).					373.800	
		Article 3 7 5	0	0	1.200.000		
	Activity 6 - Development and maintenance of EU cybersecurity						
376	***certification framework***					1.051.950	
	Activity 6 - Development and maintenance of EU cybersecurity This appropriation is intended to cover direct operational costs relevant to the Activity						6
3760			n/a	n/a	870.000	1.051.950	
	certification framework (including operational ICT and mission costs).						
		Article 3 7 6	0	0	870.000	439.900	
						439.900	

377	***Activity 7 - Supporting European cybersecurity market and industry***				
3770	Activity 7 - Supporting European cybersecurity market and industry	n/a	n/a	490.000	This appropriation is intended to cover direct operational costs relevant to the Activity 7 (including operational ICT and mission costs).
	Article 3 7 7	0	0	490.000	
378	***Activity 8 - Knowledge on emerging cybersecurity challenges and opportunities***				
3780	Activity 8 - Knowledge on emerging cybersecurity challenges and This appropriation is intended to cover direct operational costs relevant to the Activity 8 opportunities(including operational ICT and mission costs).	n/a	n/a	1.155.000	
	Article 3 7 8	0	0	1.155.000	
379	***Activity 9 - Outreach and education***				
3790	Activity 9 - Outreach and education	n/a	n/a	1.010.000	This appropriation is intended to cover direct operational costs relevant to the Activity 9 (including operational ICT and mission costs).
	Article 3 7 9	0	0	1.010.000	
	CHAPTER 3 7	**0**		**8.501.990**	
	TITLE 3	**4.868.004**		**8.888.990**	
	GRAND TOTAL	**16.932.952**	**2**	**24.207.625**	

European Union Agency
for Cybersecurity

Agamemnonos 14
Chalandri 15231 | Attiki | Greece
Tel: +30 28 14 40 9711
E-mail: info@enisa.europa.eu
www.enisa.europa.eu

Final Establishment plan 2022[1]

Category and grade	Establishment plan in voted EU Budget 2021		Establishment plan 2022	
	Off.	**TA**	**Off.**	**TA**
AD 16				
AD 15		1		1
AD 14				
AD 13		1		2
AD 12		5		4
AD 11		2		2
AD 10		3		4
AD 9		12		11
AD 8		21		23
AD 7		8		10
AD 6		4		6
AD 5				
Total AD		**57**		**63**[2]
AST 11				
AST 10				
AST 9				
AST 8		1		2
AST 7		4		3
AST 6		8		8
AST 5		5		5
AST 4		1		1
AST 3				
AST 2				
AST 1				
Total AST		**19**		**19**

[1] The change in the number of establishment plan up to 10% requested for year 2022 is modified as per Art 38 of the ENISA Financial Regulation. In 2022, ENISA will review its staffing strategy and will update a forecast for reclassification also in line with job mapping.

[2] This includes the additional 3 temporary agents, as specified in the legislative financial statement accompanying the proposal for a directive revising Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [(COM 2020/823). These resources should be managed as reserves that the Agency can draw on following the final EU adopted budget.

AST/SC1				
AST/SC2				
AST/SC3				
AST/SC4				
AST/SC5				
AST/SC6				
Total AST/SC				
TOTAL		**76**		**82**